Reminders: • k field. $(0 \neq 1)$

• A ring has an identity 1

• Any ring homomorphism send $1 \to 1$

• Subring contains 1

• Only ideals of fields are (0), (1). So any ring homomorphisms between fields are injective.

• The subfield generated by $1 \in k$ is $\{\frac{n}{m}\}$

• $k[x]$ is a PID. ($\Rightarrow$ UFD)

• $(f) = (g) \iff f = \lambda g \quad (\lambda \in k^\times)$

• $f \in k[x]$ irre ($\Leftrightarrow$ prime)

$\Leftrightarrow (f)$ prime $\Leftrightarrow (f)$ irre.

• Factor thm: $f(\alpha) = 0 \iff x - \alpha \mid f(x)$

Cor: deg n poly has most n roots.

Def: A field extension is a ring homomorphism $i: k \to K$ between fields.

denote K/k

Remark: • often i = inclusion.

• i induces an isomorphism $k \xrightarrow{\sim} i(k) \subseteq K$.

K becomes a k-vector space. (using ring operations of K)

Let $[K:k] := \dim_k(K)$ as vector space.

If $[K:k] < \infty$, say K/k a finite extension and degree $[K:k]$

Def: K/k L/k, then a k-homomorphism $K \to L$ is a ring homo $\varphi: K \to L$

s.t. $\varphi(x) = x$, $\forall x \in k$ (equivalently, k-linear)

Also have k-isomorphism

Write: $\mathrm{Hom}_k(K, L)$

Suppose K/k, $\alpha \in K$, consider evaluation (ring) homomorphism

$ev_\alpha : k[x] \to K$ (Also k-linear)

$f(x) \mapsto f(\alpha)$

$\mathrm{Image}(ev_\alpha) = k[\alpha]$ (Smallest subring containing k and α)

$\ker(ev_\alpha)$: principal

Case 1: $\ker = 0 \Rightarrow ev_\alpha : k[x] \xrightarrow{\sim} k[\alpha] \subseteq K$.

i.e. no polynomial makes $p(\alpha) = 0$, transcedental.

e.g. $t \in k(t)$

Case 2: $\ker(ev_\alpha) \neq 0 \Rightarrow \exists!$ monic polynomial $m_{\alpha,k}(x) / m_\alpha(x)$,

s.t. $\ker(ev_\alpha) = (m_\alpha(x))$

$\Rightarrow k[x]/(m_\alpha(x)) \xrightarrow{\sim} k[\alpha] \subseteq K$

$k[\alpha]$ domain $\Rightarrow (m_\alpha(x))$ prime.

In this case, α algebraic over k, $m_\alpha(x)$ minimal polynomial

(lowest degree)

Note: recall $(m_\alpha(x))$ is non-zero prime $\Rightarrow$ maximal.

$\Rightarrow k[\alpha] = k(\alpha)$ a field

We have $[k(\alpha) : k] = \dim_k(k[x]/m(x)) = \deg(m_\alpha(x))$

$k(\alpha)$ has basis $(1, \alpha, \cdots, \alpha^{\deg - 1})$

Eg: $\alpha = i$, $m_{\alpha,\mathbb{R}}(x) = x^2 + 1$, $m_{\alpha,\mathbb{C}}(x) = x - i$

If α is algebraic, we say $k[x]/(m_\alpha(x))$ is a field ext^n of k.

$k \hookrightarrow k[x] \twoheadrightarrow k[x]/(m_\alpha(x))$

Also, $k[x]/(m_{\alpha}(x)) \xrightarrow{\sim} k(\alpha)$ is a k-isom

Conversely, given $f(x)$ irre, let $k_f = k[x]/(f(x))$ a field ext^n of k.

Lemma: (1) $[k_f : k] = \deg(f)$

(2) $\bar{x} \in k_f$ is a root of the irre. poly of $f(x)$ and $k_f = k(\bar{x})$

Pf: (1) As above.

(2) Write $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.

$$f(\bar{x}) = \bar{x}^n + \cdots + a_0$$

$$= \overline{x^n + \cdots + a_0} = \overline{f(x)} = 0.$$

Every element of k_f is of the form $\sum_{i=0}^{\deg f - 1} b_i \bar{x}^i \in k(\bar{x})$, so $k_f = k(\bar{x})$

Cor: (Kronecker):

$\forall f(x) \in k[x]$ deg > 0, $\exists K/k$ s.t. $f(x)$ has a root in K.

Pf: Take $g|f$ irre, take k_g.

Prop: (Tower Law):

If $L/K/k$, then $[L:k] = [L:K][K:k]$.

Pf:
$$\begin{array}{c} L \\ | \\ K \\ | \\ k \end{array}$$

Say (α_i) basis of L/k

(β_i) basis of K/k.

WTS $(\alpha_i \beta_j)$ basis of L/k.

① spans: Take $x \in L$,

$$x = \sum \lambda_i \alpha_i \quad , \lambda_i \in K.$$

Say $\lambda_i = \sum \mu_{ij} \beta_j \quad \mu_{ij} \in k$

$$x = \sum \mu_{ij} \alpha_i \beta_j.$$

② lin. inde: Say $\sum c_{ij} \alpha_i \beta_j = 0$

$\Rightarrow \sum \alpha_i \underbrace{\left(\sum c_{ij}\beta_j\right)}_{\in k} = 0$

$\Rightarrow \forall i,j,\ \sum c_{ij}\beta_j = 0$

$\Rightarrow c_{ij} = 0.$

E.g.: • $\sqrt{2} \notin \mathbb{Q}(\sqrt[n]{2})$ $\forall n$ odd.

$\mathbb{Q}(\sqrt[n]{2})$
|
$\mathbb{Q}(\sqrt{2})$ $)n$ contradiction.
|
$\mathbb{Q}$

• If $[K:k]$ prime, then $k \subseteq L \subseteq K \Rightarrow L = K$ / $L = k$.

Prop: (Universal property of k_f)

Given any field extension $k \xhookrightarrow{i} K$, and any $\alpha \in K$ s.t. $f(\alpha) = 0$.

there exists unique ring homomorphism $k_f \xrightarrow{\varphi} K$, s.t.

$k \hookrightarrow k_f$ commutes, s.t. $\varphi(\bar{x}) = \alpha$. (can extend i uniquely from k to k_f)

$k \xhookrightarrow{i} K$

Pf: φ unique, as we know $\varphi(a) = a$ $\forall a \in k$, $\varphi(\bar{x}) = \alpha$

$\Rightarrow \varphi(\overline{\sum a_i x^i}) = \sum a_i \alpha^i$

φ exists: Consider ring homo $\tilde{\varphi} = ev_\alpha : k[x] \to K$

s.t. $\tilde{\varphi}(a) = a$, $\forall a \in k$.

As $f(\alpha) = 0$, $\tilde{\varphi}(f(\alpha)) = 0$, so by the universal property

of the quotient ring, get ring homo $\varphi : k[x]/(f(x)) \to K$

s.t. $k_f = k[x]/(f(x)) \xrightarrow{\varphi} K$ commutes.

$k[x]$ (with $k[x] \to k[x]/(f(x))$ and $k[x] \xrightarrow{\tilde{\varphi}} K$)

Then $\varphi(\bar{x}) = \alpha$, $\varphi(a) = a$ $\forall a \in k$.

Finite, algebraic field extensions.

Def: K/k is algebraic if $\forall \alpha \in K$, α is algebraic over k.

Prop: K/k finite $\Rightarrow$ K/k algebraic.

Pf: Take $\alpha \in K$, consider $1, \alpha, \alpha^2, \cdots$, they will be linearly dependent eventually.

Notation: K/k, $\alpha_i \in K$, $k(\alpha_1, \cdots, \alpha_n)$ the smallest subfield of K containing k, α_i's.

Def: K/k is finitely generated if $K = k(\alpha_1, \cdots, \alpha_n)$

K/k is simple if $K = k(\alpha)$

Prop: K/k finite $\Leftrightarrow$ algebraic + finitely (f.g.) generated

Pf: "$\Rightarrow$" fin $\Rightarrow$ alg ✓ fin $\Rightarrow$ f.g. sang $\alpha_1, \cdots, \alpha_n$ basis, $K = k(\alpha_1, \cdots \alpha_n)$.

"$\Leftarrow$" $K = k(\alpha_1, \cdots, \alpha_n)$, α_i alg over k.

$k \subseteq k(\alpha_1) \subseteq k(\alpha_1)(\alpha_2) \subseteq \cdots \subseteq k(\alpha_1, \cdots, \alpha_n) = K$.

As α_i algebraic, each layer is finite $\Rightarrow$ K/k finite.

Remark: If $\alpha_1, \cdots, \alpha_n$ algebraic $/k$, $\Rightarrow$ $k(\alpha_1, \cdots, \alpha_n)$ alg $/k$.

Prop: If $L/K/k$,

(i) L/k finite $\Leftrightarrow$ L/K, K/k finite.

(ii) L/k alg, $\Leftrightarrow$ `~~~~~` alg.

Pf: (i) Tower Law

(ii) "$\Rightarrow$" K/k alg, as $K \subseteq L$. L/K alg. as $k[x] \subseteq K[x]$.

"$\Leftarrow$" Take $\alpha \in L$, $\Rightarrow$ α alg. over K

so $\alpha^n + \cdots + a_1\alpha + a_0 = 0$, $a_i \in K$.

$\Rightarrow \alpha$ is alg. over $k(a_0, \cdots, a_{n-1})$

As $a_i \in K$ algebraic, $\Rightarrow k(a_0, \cdots, a_{n-1})/k$ f.g. algebraic $\Rightarrow$ finite.

$\Rightarrow$ $k(a_0, \cdots, a_{n-1})(\alpha)$ — finite

$k(a_0, \cdots, a_{n-1})$ — finite

k

$\Rightarrow$ Total extension is finite $\Rightarrow$ algebraic.

Algebraic closure: $\forall k$, $\exists$ "max alg. ext^n" $\bar{k}/k$, unique up to isom.

Def: A field K is alg. closed if every irred poly in $K[x]$ has deg 1

$\Leftrightarrow$ every non-constant poly has a root

$\Leftrightarrow$ every alg. ext^n of K is trivial.

Eg: $\mathbb{C}$, $\overline{\mathbb{Q}}$

Def: An alg. closure of k is $\bar{k}/k$ s.t. alg. + alg. closed.

($\Leftrightarrow$ $\bar{k}/k$ is maximal algebraic)

Eg: $\mathbb{C}/\mathbb{R}$

Thm: $\forall k$, $\bar{k}$ exists.

Pf: Consider the polynomial ring with infinitely many variables.

$A := k[X_f : f \in k[x], \deg f > 0]$

Let $I \lhd A$ generated by $f(X_f)$, $\forall f$ deg > 0

Claim: $I \neq A$ (so $\exists$ maximal ideal $\supseteq I$)

Pf: If not, $1 \in I$, i.e. $1 = \sum_{i=1}^{n} a_i f_i(X_{f_i})$, $a_i \in A$, f_i deg > 0 distinct.

By Kronecker's Thm, $\exists k'/k$ finite, s.t. $\forall 1 \le i \le n$, $\exists \alpha_i \in k'$, $f_i(\alpha_i) = 0$.

Evaluate at $X_{f_i} = \alpha_i$, then $1 = 0$

So $\exists$ maximal ideal $m \lhd I$, $m \supseteq I$, (By correspondence thm, $m \leftrightarrow \bar{m} \lhd A/I$)

Let $k_1 = A/m$. field. $k \hookrightarrow A \twoheadrightarrow A/m = k_1$

Note: Any $f \in k[x]$ has a root $\bar{x}_f$ in k_1

Iterate: $k \subseteq k_1 \subseteq k_2 \cdots$ s.t. $\forall f \in k_i[x]$, f has a root in k_{i+1}

Let $k_\infty := \bigcup_{i=1}^{\infty} k_i$. $\forall f \in k_\infty[x]$, $\exists n$ s.t. $f \in k_n[x]$

$\Rightarrow f$ has a root in $k_{n+1} \subseteq k_\infty$.

To finish, 2 ways

① Lemma: If K/k alg. closed. then $K_{alg} := \{\alpha \in K : \alpha \text{ alg.}/k\}$ is an alg. closure of k.

Pf: K_{alg} a subfield. so an alg. ext^n of k.

K alg. closed: say $f \in K_{alg}[x]$, $\exists \alpha \in K$, $f(\alpha) = 0$.

$K_{alg}(\alpha)/K_{alg}/k$ is alg. $\Rightarrow \alpha \in K_{alg}$.

② Show k_1/k alg. ($\Rightarrow k_\infty/k$ alg. by induct^n)

Point: k_1 generated by the $\bar{x}_f$, each $\bar{x}_f$ alg.

Fact: $k_1 = k_\infty$.

Prop: 1) If K/k alg., L/k, s.t. L is alg. closed, then $\exists$ k-homo. $K \xrightarrow{\varphi} L$, s.t. $K \hookrightarrow L$, $k \hookrightarrow K$, $k \hookrightarrow L$

2) If K/k, L/k alg. closures, $\varphi : K \to L$ is k-isom.

Pf: 1) Use Zorn's Lemma. $X = \{(F, \theta),\ k \subseteq F \subseteq K,\ F \xrightarrow{\theta} L,\ k \hookrightarrow F,\ k \hookrightarrow L\}$

① $X \neq 0$ since $(k, k \to L) \in X$.

Say $(F_1, \theta_1) \leq (F_2, \theta_2)$ if $F_1 \subseteq F_2$, $\theta_1 = \theta_2|_{F_1}$

NTS any chain has upper bound.

If (F_i, θ_i) is a chain (any 2 comparable), let $F' = \bigcup_{i \in I} F_i$,

and $\theta' : F' \to L$, $x \to \theta_i(x)$ if $x \in F_i$.

Check (as chain) that θ is well-defined and is an upper bound.

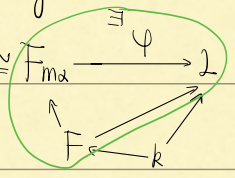
By Zorn's Lemma, $\exists$ maximal $(F, \theta) \in X$

Claim: $F = K$.

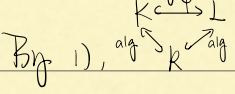
Pf: If not, take $\alpha \in K \setminus F$, then $F(\alpha)/F$ is alg.

Let $m_\alpha(x)$ be the min. poly. Let β be any root of $\theta(m_\alpha(x)) \in L[x]$ (exists since L is alg. closed)

By universal property, $F(\alpha) \cong F_{m_\alpha}$ s.t. $\psi(\alpha) = \beta$, then $(F(\alpha), \psi) > (F, \theta)$



2) K/k, L/k alg. closures.



By 1), $\Rightarrow L/k$ algebraic $\Rightarrow \psi$ isom.

Remark: If $k \subseteq K \subseteq \bar{k}$, then $\bar{k} = \bar{K}$

Splitting Fields:

Def: $f(x) \in k[x]$, $\deg > 0$, K/k field ext^n

Say f splits over K if $f(x) = c\prod_{i=1}^{n}(x - \alpha_i)$, $\alpha_i \in K$.

Say K/k is a splitting field of f if f splits over K and $K = k(\alpha_1, \cdots, \alpha_n)$

Remark: • If K is a splitting field of f over k, then K is minimal $\Leftrightarrow$ if $K/L/k$, then $K = L$.

• If L is a splitting field over k, $\exists!\ K \subseteq L$ s.t. K is a splitting field of f over k.

• A splitting field is always a finite ext^n. (has $\deg \leq n!$)

Prop: If $f(x) \in k[x]$, $\deg > 0$,

1) f admits a splitting field over k.

2) Any 2 splitting fields are k-isom.

Pf: 1) Let $\bar{k}/k$, then f splits over $\bar{k}$. So the splitting field exists by RK

2) Say K_1/k, K_2/k splitting fields of f

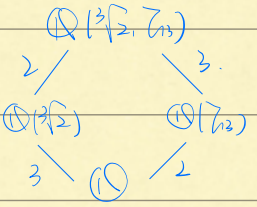
Consider $\begin{array}{ccc} \bar{K}_1 & \overset{\varphi}{\Rightarrow} & \bar{K}_2 \\ | & & | \\ K_1 & & K_2 \\ & \searrow\ k\ \swarrow & \end{array}$ So $\exists$ k-isom $\bar{K}_1 \xrightarrow{\varphi} \bar{K}_2$

Observe: if $k \le L_1 \le \bar{K}_1$ s.t. f splits over L_1,

$\Rightarrow$ $k \le \varphi(L_1) \le \bar{K}_1$ s.t. ---------- $\varphi(L_1)$

As K_i are the unique minimal fields (in $\bar{K}_i$) ✓

Eg: • Compute degrees:



• X^3-3X+1, 1) irr. 2) $\{\alpha, 1-\frac{1}{\alpha}, \frac{1}{1-\alpha}\}$ sols.

Def: Say K/k normal if $\forall \alpha \in K$, $m_{\alpha,k}(x)$ splits over K.

Eg: ①($\sqrt[3]{2}$)/① is not normal.

Thm: For K/k finite, TFAE

① K/k normal

② K/k is a splitting field of some $f(x) \in k[x]$.

③ $\forall$ k-homo $K \xrightarrow{\varphi} \bar{k}$, $\varphi(K) = K$.

Pf: ① $\Rightarrow$ ②: K/k finite $\Rightarrow$ $K = k(\alpha_1, \cdots, \alpha_n)$

Let $f(x) = \prod_{i=1}^{n} m_{\alpha_i,k}(x)$

As K/k normal $\Rightarrow$ f splits over K.

and, so ✓

② $\Rightarrow$ ③: K splitting field of f over k.

Write $f(x)=\prod_{i=1}^{n}(x-\alpha_i)$ over K.

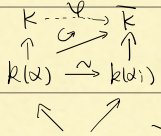
Given $\psi: K \to \bar{K}$, $\forall \alpha_i$, $f(\psi(\alpha_i)) = \psi(f(\alpha_i)) = 0$

$\Leftrightarrow \{\alpha_1, \cdots, \alpha_n\} \xleftrightarrow{\text{bij}} \{\psi(\alpha_1), \cdots, \psi(\alpha_n)\}$

$\Rightarrow \psi(K) = k(\psi(\alpha_1), \cdots, \psi(\alpha_n)) = k(\alpha_1, \cdots, \alpha_n) = K$

③ $\Rightarrow$ ① : Suppose $\alpha \in K$, Write $m_\alpha(x)=\prod_{i}^{n}(x-\alpha_i)$, $\alpha_1=\alpha$ over $\bar{K}$

$\forall i$, have k-isom, $k(\alpha_i) \cong k_{m_\alpha}^{\nsim k(\alpha)} = k[x]/m_\alpha(x)$



ψ exists by earlier prop.

In particular, $\psi: K \to \bar{K}$ a k-homo.

③ $\Rightarrow \psi(K) = K \Rightarrow \psi(\alpha) = \alpha_i \in K \Rightarrow$ ①.

Lemma: $L/K/k$, L/k normal $\Rightarrow L/K$ normal (K/k may not be)

(If L/K normal, K/k normal, $\not\Rightarrow L/k$ normal)

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

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

$\mathbb{Q}$

Pf: Use ③.

Let $\psi: L \to \bar{L}$ a K-homo,

$\Rightarrow \psi$ also a k-homo $\Rightarrow \psi(L) = L \Rightarrow L/k$ normal.

Def: Given K/k algebraic, then a normal closure is an algebraic extension N/K s.t.

① N/k normal ② If $N \geq M \geq K$ (N/K normal), N/k normal, then $N = M$.

Prop: If K/k finite, then N uniquely exists up to K-isomorphism and also finite.

Pf: Let $K = k(\alpha_1, \cdots, \alpha_n)$. Let $f(x)=\prod_{i=1}^{n} m_{\alpha_i,k}(x) \in k[x]$

Claim: N/K is a normal closure of K/k

$\Leftrightarrow N$ is a splitting field of $f(x)$ over K.

Observe: ① If $N/K/k$, N/k normal, then f splits over N.

$\Rightarrow N$ contains a splitting field of f over K.

② If S a splitting field of K, then also a splitting field of k, so S/k normal.

(Reason: $S = K(\text{roots of } f) = k(\text{roots of } f)$ since α_i's are "some" roots)

"$\Rightarrow$"

Pf claim: If N/k normal closure, then N contains the splitting field, S, of f over K, by ①.

$N/\overbrace{S/K}^{\text{normal by ②}}/k \Rightarrow N = S$

"$\Leftarrow$"

If S a splitting field of f over K, then S is normal over k by ②

If $S/\overbrace{M}^{\text{normal}}/K/k$, then f splits over M by ①. So $S = M$ by minimality of splitting field.

Separable Extension

Def: K/k alg. α is separable over k if $\min(\alpha, k)$ has no repeated roots.

Say K/k is separable if $\forall \alpha \in K$ is separable

Ex: $K = k(t^{\frac{1}{p}}) = \mathbb{F}_p(t^{\frac{1}{p}})$

$k = \mathbb{F}_p(t)$

Let $\alpha = t^{\frac{1}{p}}$ a root of $X^p - t = 0$, irreducible by Eisenstein.

Over K, $X^p - t = (X - t^{\frac{1}{p}})^p$

Lemma: If $L/K/k$, L/k separable, then L/k and K/k separable.

Pf: $m_{\alpha,K} \mid m_{\alpha,k}$

Lemma: $f(x) \in k[x]$ has repeated roots $\Leftrightarrow \gcd(f, f') \neq 1$

(If $f = \sum a_i x^i$, $f' = \sum i a_i x^{i-1}$)

Check: $(f+cg)' = f' + cg'$, $(fg)' = f'g + fg'$

Pf: $f(x) = c\prod(x-\alpha_i)$, $\alpha_i \in \bar{k}$

$\Rightarrow f'(x) = c\sum_i \prod_{i \neq j}(x-\alpha_i)$

$\Rightarrow f'(\alpha_k) = c\prod_{j \neq k}(\alpha_j - \alpha_k)$

So f have repeated root α_k

$\Leftrightarrow f'(\alpha_k) = 0$

$\Leftrightarrow f, f'$ have common root α_k.

$\Leftrightarrow x - \alpha_k \mid f, f'$ over $\bar{k}[x]$

$\Leftrightarrow m_{\alpha_k,k}(x) \mid f, f'$

So f repeated root $\Leftrightarrow \gcd(f, f') \neq 1$

Cor: If $f \in k[x]$ irr, then f has repeated roots $\Leftrightarrow f' = 0$.

Pf: repeated roots $\Leftrightarrow \gcd \neq 1$ but $\deg(f') < \deg(f)$

$\Leftrightarrow f' = 0$.

Lemma: If $\operatorname{char} k = 0$, then any alg. extension K/k is separable.

Pf: $\forall \alpha \in K$, $m_{\alpha,k}(x) = x^n + \cdots$, $m'_{\alpha,k}(x) = nx^{n-1} + \cdots \neq 0$ in $k[x]$.

Lemma: If $\operatorname{char} k = p$, $\forall f(x) \in k[x]$ irr, then $\exists r > 0$,

irr $g(x)$ with no repeated roots, s.t. $f(x) = g(x^{p^r})$

Moreover, $f(x)$ has precisely $\deg(g)$ distinct roots in $\bar{k}$,

each has multiplicity p^r.

Pf: If f has no repeated roots, done. ($r=0$, $g=f$)

Otherwise, by Cor, $f'(x)=0 \Rightarrow f'(x)=\sum i a_i x^i = 0$

$\Leftrightarrow \forall i,\ i a_i = 0$

$\Leftrightarrow a_i = 0$ or $p \mid i$, $\forall i$

$\Leftrightarrow f(x)=f_1(x^p)$ for some $f_1(x)=\sum a_{ip}x^i$

Iterate.

Write $g=\pi(x-\alpha_i) \Rightarrow f(x)=\pi(x^{p^r}-\alpha_i)$

$$=\pi(x-\alpha_i^{\frac{1}{p^r}})^{p^r}$$

Def: A field k is perfect if any f/k alg. is separable.

Def: $\mathrm{char}\, k=p>0$, Frobenius homo $\varphi: k \to k$, $x \to x^p$ ring homo.

Prop: If $\mathrm{char}\, k=p$, k perfect $\Leftrightarrow$ Frobenius homo $\varphi: k \to k$ is surjective (bijective)

Pf: k perfect $\Leftrightarrow$ every irr $f(x) \in k[x]$ has no repeated roots.

If φ surj: Say f irr in $k[x]$, $\Rightarrow f(x)=g(x^{p^r})$

$g(x)=\sum b_i x^i \Rightarrow f(x)=\sum b_i x^{ip^r}$

$\Rightarrow f(x)=\sum \left((b_i^{\frac{1}{p^r}})x\right)^{p^r}$ ($\exists \in k$ as φ surj)

$=\left(\sum (b_i^{\frac{1}{p^r}})x\right)^{p^r}$

reducible if $r \neq 0$

So $r=0$, $f=g$, f has no repeated roots.

If φ not surj: Take $\alpha \notin \varphi(k)$, i.e. $\alpha \in k \setminus k^p$

The minimal poly of $\alpha^{\frac{1}{p}} \in \bar{k} \setminus k$ divides $(X^p - \alpha) \in k[X]$.

$X^p - \alpha = (X - \alpha^{\frac{1}{p}})^p$ in $\bar{k}[X]$.

If k perfect, $m_{\alpha^{\frac{1}{p}}, k}(X) = X - \alpha^{\frac{1}{p}} \notin k[X]$. contradiction.

Eg: in $k = \mathbb{F}_p(t)$, $t \in \psi(k)$

Cor: finite fields are perfect

Pf: ψ injective.

Def: K/k alg. $[K:k]_s := |\mathrm{Hom}_k(K, \bar{k})|$ the separable degree.

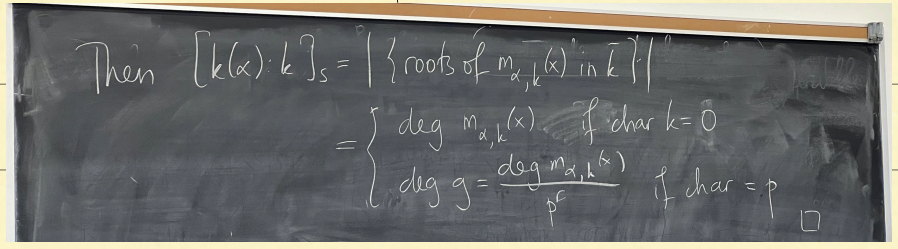
Prop: If α alg $/k$, $[k(\alpha):k] = \begin{cases} [k(\alpha):k]_s & \text{if } \mathrm{char}\, k = 0 \\ p^r [k(\alpha):k]_s & \text{if } f(x) = g(x^{p^r}) \end{cases}$

In particular, $[k(\alpha):k]_s \mid [k(\alpha):k]$, eqnl $\Leftrightarrow \alpha$ separable

Pf: $k(\alpha) \cong k[x]/(m_{\alpha,k}(x))$, by universal property of $k[x]$,

$|\mathrm{Hom}_k(k(\alpha), \bar{k})| \longleftrightarrow \{$ roots of $m_{\alpha,k}(x)$ in $\bar{k}\}$.

$\psi \longleftrightarrow \psi(\alpha)$



Prop: If $L/K/k$ finite, then $[L:k]_s = [L:K]_s [K:k]_s$.

Pf: NTS $\mathrm{Hom}_k(L, \bar{k}) \cong \mathrm{Hom}_K(L, \bar{k}) \oplus \mathrm{Hom}_k(K, \bar{k})$

τ_j $\quad$ σ_i

Extend σ_i: $\begin{array}{ccc} & & \bar{k} \\ & \nearrow^{\tilde{\sigma}_i} & \uparrow \\ L & \xrightarrow{\sigma_i} & \bar{L} \\ \uparrow & & \uparrow \\ K & \xrightarrow{\sim} & K \\ \uparrow & & \uparrow \\ k & \xrightarrow{\sim} & k \end{array}$

By uniqueness of alg. closure, $\tilde{\sigma}_i$ is an isom.

$\forall \psi \in LHS$, Then $\psi|_k = \sigma_i$ for some i.

$\tilde{\sigma}_i^{-1} \circ \psi|_k$ = inclusion from $k \to \bar{L}$

$\Rightarrow \tilde{\sigma}_i^{-1} \circ \psi \in \mathrm{Hom}_k(L, \bar{L}) \Rightarrow \tilde{\sigma}_i^{-1} \circ \psi = \tau_j$, some j.

So $\psi = \tilde{\sigma}_i \circ \tau_j$.

Remains to show: $\tilde{\sigma}_i \circ \tau_j = \tilde{\sigma}_l \circ \tau_m \Rightarrow i=l,\ j=m$.

Restrict to k: $\tilde{\sigma}_i|_k = \tilde{\sigma}_l|_k \Rightarrow \sigma_i = \sigma_l$.

$\Rightarrow \tau_j = \tau_m \Rightarrow j = m$.

Prop: If K/k finite,

① $[K:k] = \begin{cases} [K:k]_s & \text{if } \mathrm{char}\, k = 0 \\ p^r [K:k]_s & \text{if } \mathrm{char}\, k = p, \text{ for some } r. \end{cases}$

② $[K:k]_s = [K:k] \iff K/k$ separable.

Pf: ①:

$K = k(\alpha_1, \cdots, \alpha_n)$

$k(\alpha_1, \cdots, \alpha_{n-1})$

$\vdots$

k

② "$\in$": each $k(\alpha_1, \cdots, \alpha_n)/k(\alpha_1, \cdots, \alpha_{n-1})$ separable ✓

"$\Rightarrow$": $\forall \alpha \in K$, consider $\begin{matrix} K \\ | \\ k(\alpha) \\ | \\ k \end{matrix}$.

So $[k(\alpha):k]_s = [k(\alpha):k]$.

Cor: $L/k/k$ finite, $L/k/k$ separable $\iff L/k$, K/k separable

Pf: ② + Tower law.

Prop: (Primitive element thm)

If K/k finite + separable, then $K = k(\alpha)$ for some $\alpha \in K$.

Remark: Fails if inseparable.

Pf: Case 1: If k finite, then K finite.

$\Rightarrow K^+$ is cyclic $= \langle \alpha \rangle$.

So $K = k(\alpha)$

Case 2: $K = k(\alpha_1, \cdots, \alpha_n)$. WLOG $K = k(\alpha, \beta)$

If k is infinite, $[K:k]_s = [K:k] = n$

Write $\mathrm{Hom}_k(K, \bar{k}) = \{\sigma_1, \cdots, \sigma_n\}$

Trick: Let $f(x) = \prod_{i \neq j} \left((\sigma_i(\alpha) - \sigma_j(\alpha)) + (\sigma_i(\beta) - \sigma_j(\beta))x \right)$

① $(\sigma_i(\alpha) - \sigma_j(\alpha)) + (\sigma_i(\beta) - \sigma_j(\beta))x \neq 0$

if $=0$, then $\sigma_i(\alpha) = \sigma_j(\alpha)$, $\sigma_i(\beta) = \sigma_j(\beta)$, then $\sigma_i = \sigma_j$.

So $f \neq 0 \Rightarrow \exists c \in k$, $f(c) = 0$. (since k infinite)

$\Rightarrow (\sigma_i(\alpha) - \sigma_j(\alpha)) + (\sigma_i(\beta) - \sigma_j(\beta))c \neq 0$

$\Rightarrow \sigma_i(\alpha + c\beta) \neq \sigma_j(\alpha + c\beta)$ (since $c \in k$)

$\mathrm{Hom}_k(k(\alpha + c\beta), \bar{k})$ has $\geq n$ elements.

So $[K:k] \geq [k(\alpha + c\beta) : k] \geq [k(\alpha + c\beta) : k]_s \geq n$.

Galois Theorem

Def: K/k is Galois if Normal + Separable.

Remark: L/k. if L/k Galois, then L/k Galois.

Def: For K/k, define $\mathrm{Aut}_k(K) = \mathrm{Isom}_k(K, K)$

For K/k Galois, $\mathrm{Gal}(K) = \mathrm{Aut}_k(K) = \mathrm{Isom}_k(K, K)$

Prop: If K/k finite, then $|\mathrm{Aut}(K)| \leq [K:k]$, with equality

iff K/k Galois.

Pf: Note $Aut_k(K) = Isom_k(K,K) \leq Hom_k(K,\bar{k})$

$\Rightarrow |Aut_k(K)| \leq |Hom_k(K,\bar{k})| = [K:k]_s \leq [K:k]$.

($\leq$: Normal; $[K:k]_s \leq [K:k]$: Separable)

Cor: If K/k finite Galois, then $|Gal(K/k)| = [K:k]$

Def: An intermediate field of K/k is L s.t. $k \leq L \leq K$.

Galois Correspondence: Fix K/k Galois.

$$\{\text{Intermediate field}\} \underset{\Phi}{\overset{\Theta}{\rightleftarrows}} \{\text{Subgroups of } Gal(K)\}$$

$$F \longmapsto Gal(K/F) = \{g \in Gal \mid g(F) = F \text{ pointwise}\}.$$

$$\{\alpha \in K \mid h(\alpha) = \alpha \ \forall h \in H\} = K^H \longleftarrow H$$

Goal: Θ, Φ are inverse bijections.

Basic observation:

① Θ, Φ are order-reversing, i.e.

$F_1 \subseteq F_2 \Rightarrow \Theta(F_1) \geq \Theta(F_2)$

$\Phi(H_1) \geq \Phi(H_2) \Leftarrow H_1 \leq H_2$.

② $\Phi(\Theta(F)) = K^{Gal(K/F)} \supseteq F$

$\Theta(\Phi(H)) = Gal(K/K^H) = H$

③ = ① + ② $\Rightarrow \Theta(\Phi(\Theta(F))) = \Theta(F)$,

$\Phi(\Theta(\Phi(H))) = \Phi(H)$.

④ If F is any intermediate field, then K/F is galois

$\Rightarrow |Gal(K/F)| = [K:F]$

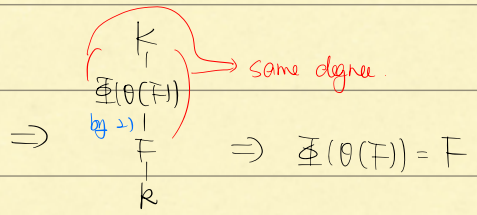
$\|$

$|\Theta(F)|$

⑤ Apply 3) + 4), $|\Theta(\Phi(\Theta(F)))| = |\Theta(F)|$

$\|$

$[k : \Phi(\Theta(F))] = [k : F]$



$\Rightarrow \Phi(\Theta(F)) = F$

In particular, Θ is injective.

Cor: A finite galois extension has only finitely many intermediate fields.

Remark: Same is true for any finite separable extension (idea: Consider the normal closure).

Fails for inseparable extensions.

Prop: Suppose K is any field, G any finite subgroup of field automorphisms of K, i.e. $G \leq Aut(G)$

Then K/K^G is finite galois with $Gal(K/K^G) = G$ (inside $Aut(K)$).

Pf: Next time.

Cor: If K/k finite Galois, then $\Theta \cdot \Phi = id$. i.e. $Gal(K/K^H) = H$, $\forall H \leq Gal(K/k)$

Thm (Fundamental Thm of Galois Theory):

K/k finite Galois.

(1) Θ, Φ are inverse + order-reversing bijections.

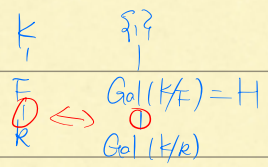
$$\{\text{int. fields of } K/k\} \longleftrightarrow \{\text{subgroups of } Gal(K/k)\}.$$

(2) If $F \longleftrightarrow H$ (in (1)),

then $[k:F] = |H|$

(3) Also, if $F \longleftrightarrow H$ (in (1))

F/k normal $\Leftrightarrow H \trianglelefteq Gal(k/k)$



Moreover, in that case, $Gal(F/k) \cong Gal(k/k)/H$

K/k finite

Galois if normal + sep $\Leftrightarrow |Aut_k(k)| = [k:k]$ ($\leq$ in general)

$Gal(k/k)$.

Thm above

Picture galois: $k \Leftrightarrow 1$, $F \Leftrightarrow H$, $k \Leftrightarrow G$ — order-reversing.

Remark/exercise: • If $F_1 \supset F_2 \Leftrightarrow H_1 \subset H_2$, then F_1/F_2 is normal $\Leftrightarrow H_1 \trianglelefteq H_2$, and $Gal(F/F_2) \cong H_2/H_1$

In general, $[F_1:F_2] = (H_2:H_1)$

• If F_1, F_2 are intermediate fields, $F_i \Leftrightarrow H_i$,

then $F_1 \cap F_2 \longleftrightarrow \langle H_1, H_2 \rangle$

Point: Θ, Φ are order reversing

Recall: Showed $\Phi \circ \Theta = id$

For $\Theta \circ \Phi = id$,

Prop: k field, $G \leq Aut(k)$ finite, then K/K^G (K^G = fixed by G) is galois with galois group $Gal(K/K^G) = G$.

Pf: Note that G acts on K (as a set) ($G \curvearrowright X$ acting $\Leftrightarrow G \to S_X$ homo, $Aut\, K \leq S_K$)

NTS normal/separable.

Pick $\alpha \in K$. Let $f(x) = \prod_{\beta \in G\cdot\alpha} (x-\beta) \in K[x]$. (orbit of α)

Claim: $f(x) \in K^G[x]$.

Pf: Enough to show $\sigma(f(x)) = f(x)$ $\forall \sigma \in G$ (acting on every coefficient.)

$\sigma(f(x)) = \prod_{\beta \in G\cdot\alpha} (x - \sigma(\beta)) = \prod (x-\beta) = f(x)$ (permutes roots)

Why minimal?

Claim: $f(x)$ is the minimal polynomial over K^G.

① $m_\alpha(x) \mid f(x)$ $f(\alpha)=0$ and $f(x) \in K^G[x]$.

② $f(x) \mid m_\alpha(x)$ since $x-\alpha \mid m_\alpha(x)$ in $K[x]$

$\Rightarrow x - \sigma(\alpha) \mid \sigma(m_\alpha(x)) = m_\alpha(x)$

$\Rightarrow \prod (x-\sigma(\alpha)) = f(x) \mid m_\alpha(x)$

no repeated roots

Claim shows α is normal + separable $/K^G$. $(\forall \alpha \in K)$

So K/K^G is galois.

and $[K^G(\alpha) : K^G] = |G\alpha| \leq |G|$. (if finite, we can write $K = K^G(\alpha)$ but don't know)

To see K/K^G finite,

Pick $K/F/K^G$ Finite with $[F:K^G]$ maximal.

F exists because F/K^G finite $\Rightarrow \leq |G|$.

If $F \subsetneq K$, then $\exists \beta \in K \setminus F$,

$F(\beta) \supsetneq F \supset K^G$

finite

finite because β alg $/K^G$.

contradiction.

So $F = K$, i.e. K/K^G finite.

Now $G \leq \underbrace{\mathrm{Aut}(K/K^G)}_{\leq |G| \text{ (above)}} (\leq \mathrm{Aut}(K))$

$\Rightarrow G = \mathrm{Gal}(K/K^G)$

■

Cor: If K/k finite Galois, then $m_{\alpha}(x) = \prod_{\beta \in G\alpha} (x-\beta)$

Pf of FTGT: (1) done

(2) if $F \leftrightarrow H$, then $H = Gal(K/F) \Rightarrow |H| = [K:F]$

(3)

Lemma: If F is an intermediate field, then F/k galois (normal)

$\iff \sigma(F) = F, \forall \sigma \in G.$

Remark: $\sigma: K \xrightarrow{\sim} K$, so $\sigma(F)$ is another intermediate field.

Pf: "$\Rightarrow$"

If F/k normal, then pick $\alpha \in F$ and $\sigma \in G$

ETS: $\sigma(\alpha) \in F$

Then $m_{\alpha,k}(x)$ splits/F, and $m_{\alpha,k}(\alpha) = 0$

$\Rightarrow \sigma(m_{\alpha,k}(\alpha)) = m_{\alpha,k}(\sigma(\alpha)) = 0$

"$\Leftarrow$"

If $\sigma(F) = F$

group homo $G \to Aut(F)$, $\sigma \mapsto \sigma|_F$

with kernel $Gal(K/F) = H \trianglelefteq G$.

So $G/H \leq Aut(F)$ (finite)

by prop earlier, $F/F^{(G/H)}$ is finite galois with galois group G/H.

$F^G = k$ (As $k^q = k$)

Pf of (3): $F \leftrightarrow H$ as in (1)

Observe: $\sigma(F) \leftrightarrow \sigma H \sigma^{-1}$ (for $\sigma \in G$)

($x \in F$, $h(x) = x$; $\sigma h \sigma^{-1}(\sigma(x)) = \sigma(h(x)) = \sigma(x)$)

Then F/k normal $\overset{\text{Lemma}}{\iff} \sigma(F) = F \ \forall \sigma \in G$

$\Leftrightarrow H = \sigma H \sigma^{-1} \quad \forall \sigma \in G.$

$\Leftrightarrow H \lhd G.$

In that case, $G \longrightarrow Gal(F/k)$

$\| \quad$ by def

$Gal(K/F)$

$\sigma \longmapsto \sigma|_F$ well-defined because $\sigma(F) = F$ + group homo.

Kernel $= Gal(K/F) = H \lhd G.$

$\Rightarrow G/H \cong im(\varphi) \leq Gal(F/k)$

$Gal(F/k) = [F:k] = \frac{[K:k]}{[K:F]} = \frac{|G|}{|H|}$ so φ iso ■

Example: $K = \mathbb{Q}_{x^4-2} = \mathbb{Q}(\sqrt[4]{2}, i)$

K — 2 — $\mathbb{Q}(\sqrt[4]{2})$ — 2 — $\mathbb{Q}$ — 4

$K/\mathbb{Q}$ Galois (as separable + char = 0)

Compute Gal group: $|G| = 8$

$\sigma \in G. \Rightarrow \sigma(i) = \pm i$ as root of x^2+1

$\sigma(\sqrt[4]{2}) \in \{ i^k \cdot \sqrt[4]{2} \}$ as root of x^4-2.

σ is determined by values on generators. $\Rightarrow |G| \leq 8$

So all in G

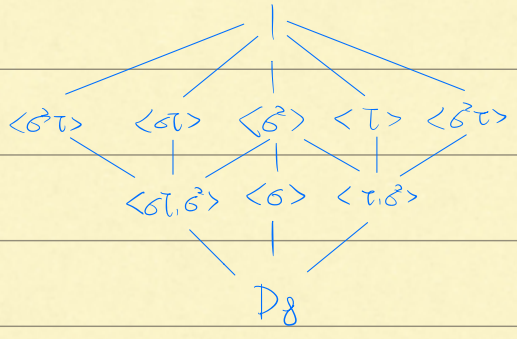
$\Rightarrow$ get $\begin{cases} \sigma(\sqrt[4]{2}) = i\sqrt[4]{2} \\ \sigma(i) = i \end{cases}$ order 4

$\begin{cases} \tau(\sqrt[4]{2}) = \sqrt[4]{2} \\ \tau(i) = -i \end{cases}$ order 2.

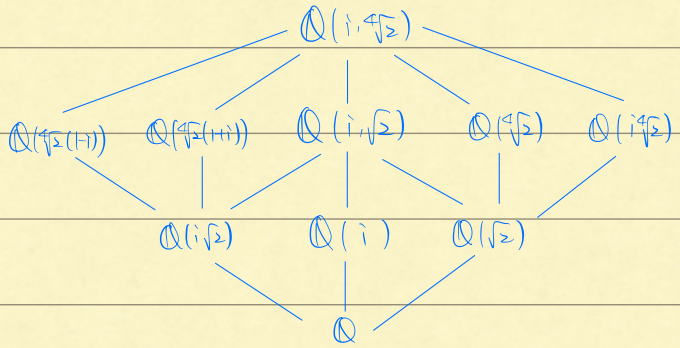
$\sigma\tau = \tau\sigma^{-1}$, $\sigma^4, \tau^2 = 1$. So get D_8.

(and $G = \langle \sigma, \tau \rangle$).

Subgroup lattice:



Intermediate field:



Finite fields:

If k a finite field, prime subfield $\mathbb{F}_p$ (some prime)

$\rightarrow |k| = p^r$, $r = \dim_{\mathbb{F}_p}(k) = [k:\mathbb{F}_p]$.

Prop: $q = p^r = |k|$, $\forall n \geq 1$, $\exists$ unique (up to k-isom) extension of degree n.

Then $|K| = q^n$, $Gal(K/k) = \langle \varphi^r : x \mapsto x^q \rangle$ is cyclic order n.

Pf: Suppose K/k such an extension, $(\Rightarrow |K| = q^n)$

Then $K^\times$ cyclic of order $q^n - 1$, i.e, $\alpha^{q^n-1} = 1 \Leftrightarrow \alpha^{q^n} = \alpha$, $\forall \alpha$.

$\Rightarrow f(x) = X^{q^n} - X = \prod_{\alpha \in k} (X - \alpha)$ so K is the splitting field of $f(x)$ over k.

So K normal, unique up to k-isom.

K/k separable since $f(x)$ separable

$\Rightarrow K/k$ Galois of deg n. $\Rightarrow |Gal(K/k)| = n$.

Claim: $\varphi^r \in Gal(K/k)$ and has deg n.

Pf: ① $\varphi^r : x \to x^q$ fix $\forall \alpha \in k$ since $x^q = x$ $\forall \alpha \in k$.

② Suppose $(\varphi^r)^i = id$ on k,

$\Leftrightarrow \alpha \to \alpha^{q^i} = \alpha$, $\forall \alpha \in k$. $i \geq n$.

remains to show existence:

Fix n. Let $K :=$ splitting field of $x^{q^n} - x$ over k

Note: K is also the splitting field of $x^{q^n} - x$ over $\mathbb{F}_p$.

Let $k' = \{\alpha \in K : \alpha^{q^n} = \alpha \Leftrightarrow \varphi^n(\alpha) = \alpha\}$ (since K split fld, smallest)

As φ a ring homo, k' is a subfield of K, so $k' = K$.

$|k'| = q^n$ as $f'(x) = -1$, ✓

Cor: $\forall n \geq 1$, there is a unique field of size $q = p^n$ up to isom.

Eg: ① $\mathbb{F}_2[x]/x^2+x+1 = \mathbb{F}_4$

② $\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$

Solvability by radicals (Assume char $k = 0$)

Idea: $f = k[x]$ is solvable in radicals if its roots can be obtained from k using field operations and $\sqrt[n]{\ }$

Def: A finite extension K/k is radical if

$\exists\, k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_r$ s.t. $k_{i+1} = k_i(\alpha_i)$, $\alpha_i^{n_i} \in k_i$,

and $K \subseteq k_r$.

So f is solvable by radicals if $\exists\, K/k$ radical s.t. f splits over k.

Goal: f is solvable by radicals $\Leftrightarrow$ $\mathrm{Gal}(K/k)$ solvable.

Recall: G solvable if $\exists\, 1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$

G_i/G_{i-1} abelian $\Leftrightarrow$ cyclic.

Def: K/k is abelian / cyclic if K/k Galois and $\mathrm{Gal}(K/k)$ is abelian / cyclic

接下一个 lemma.

Thm: If K/k finite Galois.

K/k radical $\Leftrightarrow$ $\mathrm{Gal}(K/k)$ solvable.

Lemma1: Let K be the splitting field of x^n-1 over k,

then K/k abelian.

Pf: K/k Galois. $f(x)=x^n-1$, $f'(x)=nx^{n-1}$ $\Rightarrow f$ no repeated roots.

$\Rightarrow |\mu_n(k)|=n$, say $\mu_n(k)=\langle \zeta_n \rangle$.

For $\sigma \in \mathrm{Gal}(K/k)$, $\sigma(\zeta_n)$ is still a primitive root, so

$\sigma(\zeta_n)=\zeta_n^{\theta(\sigma)}$, where $\theta(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$

Then note: $\theta: \mathrm{Gal}(K/k) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is a group homomorphism.

And θ is injective, so $K=k(\zeta_n)$.

$\Rightarrow \mathrm{Gal}(K/k) \leq (\mathbb{Z}/n\mathbb{Z})^\times$ abelian.

Lemma2: Suppose $\zeta_n \in k$ $(\Leftrightarrow |\mu_n(k)|=n)$

If $K=k(\alpha)$, $\alpha^n \in k$, then K/k cyclic.

Pf: If $\alpha \neq 0$, K/k is splitting field of $x^n-\alpha^n$.

$\Rightarrow K/k$ is normal, so Galois.

If $\sigma \in \mathrm{Gal}(K/k)$, $\sigma(\alpha)=\alpha\zeta_n^{\psi(\sigma)}$, some $\psi(\sigma) \in \mathbb{Z}/n\mathbb{Z}$.

Check: $\psi: \mathrm{Gal}(K/k) \longrightarrow \mathbb{Z}/n\mathbb{Z}$ ($\sigma \longmapsto \psi(\sigma)$) is an injective group homo. (as before)

$$\alpha\cdot\zeta_n^{\psi(\sigma\tau)}=\sigma(\tau(\alpha))=\sigma(\alpha\zeta_n^{\psi(\tau)})=\sigma(\alpha)\cdot\zeta_n^{\psi(\tau)}=\alpha\cdot\zeta_n^{\psi(\sigma)+\psi(\tau)} \quad (\zeta_n \in k)$$

Def (Non-standard): M/k finite is polyabelian if

$\exists\, k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_r = M$ s.t. k_i/k_{i-1} abelian.

Remark: K/k polyab + Galois $\overset{\text{FTGT}}{\Longrightarrow}$ $\mathrm{Gal}(K/k)$ solvable.

Lemma: (i) If $\begin{matrix} & K & \\ E & & F \\ & k & \end{matrix}$, E/k, F/k, then EF/k also polyab.

(ii) If K/k is polyab with normal closure $N/k \Rightarrow N/k$ polyab.

Pf: (i) As polyab, $k = k_0 \subseteq \cdots \subseteq k_r = E$, $k = k_0' \subseteq \cdots \subseteq k_s' = F$.

So $k = k_0 \subseteq \cdots \subseteq k_r = E = Ek_0' \subseteq Ek_1' \subseteq \cdots \subseteq Ek_s' = EF$.

NTS Ek_j'/Ek_{j-1}' abelian.

① Ek_j'/Ek_{j-1}' is Galois by HW1

② $\mathrm{Gal}(Ek_j'/Ek_{j-1}') \xrightarrow{\theta} \mathrm{Gal}(k_j'/k_{j-1}')$, $\sigma \longmapsto \sigma|_{k_{j-1}'}$

(Note $\sigma(k_j') = k_j'$ As k_j'/k_{j-1}' normal)

(Also θ is inj as $Ek_{j-1}' \cdot k_j' = Ek_j'$

$\Rightarrow \mathrm{Gal}(Ek_j'/Ek_{j-1}') \leq \mathrm{Gal}(k_j'/k_{j-1}')$

ab. $\Leftarrow$ ab

(ii) $G = \mathrm{Gal}(N/k)$

Claim: $N = \underbrace{\langle \sigma(K) \mid \sigma \in G \rangle}_{M}$ compositum ($\Rightarrow$ done by (i))

As G permutes $\{\sigma(K)\}$, say G stabilize M, i.e. $\sigma(M) = M$, $\forall \sigma$.

$\Rightarrow M/k$ normal

Minimality of $N \Rightarrow N = M$.

Pf of Thm: "$\Longrightarrow$"

K/k Galois + radical

$\Rightarrow k = k_0 \subseteq \cdots \subseteq \overset{K}{k_r}$, $k_i = k_{i-1}(\alpha_i)$, $\alpha_i^{n_i} \in k_{i-1}$

Let $N = \mathrm{lcm}(n_1, \cdots, n_r)$. working inside k_r, pick $\zeta_N = \sqrt[N]{1}$ primitive.

$k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_r$ $\quad k_j(\zeta_N) \subseteq k_{j+1}(\zeta_N)$ cyclic by lemma 2.

$k_0(\zeta_N) \subseteq \cdots \subseteq k_r(\zeta_N)$ $\quad k_0 \subseteq k_0(\zeta_n)$ abelian.

So $k_r(\zeta_N)/k$ polyabelian.

So N/k polyab as N the normal closure of $k_r(\zeta_N)/k$.

FTGT $\Rightarrow$ $\mathrm{Gal}(N/k)$ solvable. $\Rightarrow$ its quotient group solvable.

Note $\begin{matrix} N \\ | \\ k_r(\zeta_N) \\ | \\ k \end{matrix}$ Galois $\Rightarrow$ $\mathrm{Gal}(k/k)$ is a quotient group of $\mathrm{Gal}(N/k)$. $\surd$

Galois $\Rightarrow$ "$\Leftarrow$"

Lemma: (linear independence of characters)

F any field. G any group,

$\chi_1, \cdots, \chi_r$ $G \to F^\times$ distinct group homs.

Then $\chi_1, \cdots, \chi_r$ linearly independent over F.

i.e, if $\sum_1^r \lambda_i \chi_i(g) = 0$ $\forall g$ $\Rightarrow \lambda_i = 0$ $\forall i$

Pf: If not, take a minimal counter example.

Say $(\lambda_1\chi_1 + \cdots + \lambda_r\chi_r)(g) = 0$, $\forall g$.

$\lambda_1\chi_1(gN) + \cdots + \lambda_r\chi_r(gN) = 0$, $\forall g \forall h$.

$\cdot \chi_1(h)$ $\lambda_1\chi_1(g)\chi_1(h) + \cdots + \lambda_r\chi_r(g)\chi_r(h) = 0$ ①

$\lambda_1\chi_1(g)\chi_1(h) + \cdots + \lambda_r\chi_r(g)\chi_1(h) = 0$. ②

① − ② $\Rightarrow$ $\lambda_2(\chi_2(h) - \chi_1(h))\chi_2(g) + \cdots + \lambda_r(\chi_r(h) - \chi_1(h))\chi_r(g) = 0$.

Choose h s.t. $\chi_2(h) - \chi_1(h) \neq 0$. Contradiction.

Lemma: (Hilbert 90) K/k finite cyclic deg n, with σ a generator of $\mathrm{Gal}(K/k)$.

If $\prod_{i=0}^{n-1} \sigma^i(\alpha) = 1$ $\overset{\text{Norm}}{\Leftrightarrow}$ then $\alpha = \frac{\beta}{\sigma(\beta)}$ for some $\beta \in K^\times$

Pf: By Dedekind, $1, \sigma, \sigma^2, \cdots, \sigma^{n-1}: K^\times \to K^\times$ are linearly independent. So the linear combination

$$\sigma^0 + \alpha\cdot\sigma^1 + \alpha\cdot\sigma(\alpha)\cdot\sigma^2 + \cdots + \alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-2}(\alpha)\cdot\sigma^{n-1} \neq 0.$$

So $\exists\, \gamma \in K^\times$, $\beta = \gamma + \alpha\sigma(\gamma) + \alpha\sigma(\alpha)\sigma^2(\gamma) + \cdots + \alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(\gamma) \neq 0$

$$\sigma(\beta) = \sigma(\gamma) + \sigma(\alpha)\sigma(\gamma) + \sigma(\alpha)\sigma^2(\alpha)\sigma^2(\gamma) + \cdots + \sigma(\alpha)\cdots\sigma^{n-1}(\alpha)\sigma^n(\gamma) = \gamma$$

$\Rightarrow \alpha\cdot\sigma(\beta) = \beta$ as $\alpha\cdot\sigma(\alpha)\cdots\sigma^{n-1}(\alpha) = 1$ by assumption. ✓

Lemma: If $\zeta_n \in k$ and K/k is cyclic of deg n then $\exists \alpha \in K$, s.t. $K = k(\alpha)$ and $\alpha^n \in k$.

Pf: $\mathrm{Gal}(K/k) = \langle\sigma\rangle$.

Apply Hilbert 90 to $\zeta_n \in k$, (As $N_m(\zeta_n) = 1$)

By Hilbert, $\zeta_n = \alpha/\sigma(\alpha)$, some $\alpha \in K^\times$

i.e. $\sigma(\alpha) = \alpha\zeta_n^{-1}$

$\overset{\text{Induction}}{\Rightarrow}$ $m_{\alpha,k}(x)$ has roots at least $\alpha\cdot\zeta_n^i$ $(0 \le i \le n-1)$

But $[K:k] = n$, so $\deg m_{\alpha,k}(x)$, so $K = k(\alpha)$

Finally $\sigma(\alpha^n) = \alpha^n \Rightarrow \alpha^n \in k$.

Pf: ("$\Leftarrow$")

Suppose K/k finite Galois with $\mathrm{Gal}(K/k)$ solvable.

FTGT $\Rightarrow$ $k = k_0 \le k_1 \le \cdots \le k_r = K$, k_i/k_{i-1} normal, cyclic.

Let $d := [K:k]$, $d_i := [k_i : k_{i-1}]$

Consider inside $\bar{k}$, $k = k_0 \le k_1 \le \cdots \le k_r$

$$k(\zeta_d) \le \cdots \le k_r(\zeta_d)$$

Note $k_i(\zeta_d)/k_{i-1}(\zeta_d)$ is cyclic with degree dividing d_i (therefore d)

Lemma $\Rightarrow$ $k_i(\zeta_d) = k_{i-1}(\zeta_d)(\alpha_i)$, with $\alpha_i^{d_i'} \in k_{i-1}$

So $k = k_0 \le k_0(\zeta_d) \le k_1(\zeta_d) \le \cdots \le k_r(\zeta_d)$. So $K \le k_r(\zeta_d)$, radical.

Suppose $f(x) \in k[x]$ irred, deg n, let N be a splitting field of f over k, N/k Galois

$G := Gal(N/k)$ acts transitively and faithfully on $\{\alpha_1, \dots, \alpha_n\}$ roots of f in N $\{=X\}$

$\Rightarrow G \hookrightarrow S_X \cong S_n$ injective ($\Leftrightarrow$ faithful) $\Rightarrow G \leq S_n$

Prop: $f(x) = X^5 - 4x + 2 \in \mathbb{Q}[x]$ not solvable by radicals.

Pf: We'll show $G = S_5$ in this case, not solvable $\Rightarrow$ not radical.

Claim 1: G contains a 2-cycle.

First show $f(x)$ has 3 real roots.

$f'(x) = 5x^4 - 4$ has only 2 roots in $\mathbb{R}$, so f has ≤ 3 real roots in $\mathbb{R}$.

$f(\pm\infty) = \pm\infty$, $f(0) > 0$, $f(1) < 0$ $\Rightarrow$ 3 real roots.

WLOG, $N \subseteq \mathbb{C}$, then complex conjugation $\tau : \mathbb{C} \to \mathbb{C}$ sends N to N

$\Rightarrow \tau|_N \in Gal(N/k)$ is a 2-cycle.

Claim 2: G contains a 5-cycle.

N

$|$

$\mathbb{Q}(\alpha)$ α root of f

$|$ deg 5 by eisen

$\mathbb{Q}$ $\Rightarrow 5 \mid [N:\mathbb{Q}] = |G| \Rightarrow \exists$ element in G of order 5.

$\Rightarrow G$ has a 5-cycle.

Claim 3: $\forall H \leq S_5$ containing 2-cycle and 5-cycle, then $H = S_5$

We know all 2-cycle generates S_5.

WLOG, (12), (12345)

Remark: transitive subgroups of S_5:

$\mathbb{Z}_5 \times \mathbb{Z}_4$

C_5, D_{10}, F_{20}, A_5, S_5 (All possible)

- $\mathbb{Q}(\zeta_n)$ / $\mathbb{Q}$ $\quad Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism.

Thm: (Kronecker-Weber):

If $K/\mathbb{Q}$ finite abelian, then $K \subseteq \mathbb{Q}(\zeta_n)$ for some n.

Commutative Algebra

Noetherian rings/modules:

R ring (maybe not commutative, always $1 \in R$)

M: left R-module.

Ascending chain condition: (ACC)

If $M_1 \subseteq M_2 \subseteq \cdots$, then $\exists n \geq 1$, s.t. $M_n = M_{n+1} = \cdots$

Def: A R-module M is noetherian if it satisfies ACC for submodules.

ring R is noetherian if it satisfies ACC for left ideals.

$\Leftrightarrow$ (R as a left R-module).

Lemma: TFAE:

① M noetherian

② every submodule of M are f.g.

Pf: ① $\Rightarrow$ ②: if $N \subseteq M$, take $x_1 \in N \setminus \{0\}$.

If $N = Rx_1 = \{rx_1\}$, done

otherwise, $x_2 \in N \setminus Rx_1$, keep going.

② $\Rightarrow$ ①: Say $M_1 \subseteq M_2 \subseteq \cdots$ AC for submodules.

Let $N := \bigcup M_i$ still submd

N is fg $\Rightarrow N = Rx_1 + \cdots + Rx_k$.

Say $x_i \in M_{n(i)} \Rightarrow x_1, \ldots, x_k \in M_{\max\{n_i\}} = N$

$\Rightarrow M_n = M_{n+1} = \cdots$

Cor: ring R noe $\Leftrightarrow$ every left ideal is fg.

Ex: ~~Any~~ PID noe.

$k[x_1, \ldots, x_n, \ldots]$ not noe.

Lemma: If $N \subseteq M$, then

M noe $\Leftrightarrow N$ and M/N noe.

Pf: "$\Rightarrow$" N noe: every Ac of N is a Ac of M.

M/N noe: $\bar{M}_1 \subseteq \bar{M}_2 \subseteq \cdots$ Ac for M.

"$\Leftarrow$" Say $M_1 \subseteq M_2 \subseteq \cdots$

$\Rightarrow$ $M_1 \cap N \subseteq M_2 \cap N \subseteq \cdots$, $\pi(M_1) \subseteq \pi(M_2) \subseteq \cdots$ $\Rightarrow$ $M_n \cap N = M_{n+1} \cap N$, $\pi(M_n) = \pi(M_{n+1}) \Rightarrow M_n + N = M_{n+1} + N$.

Claim: $M_n = M_{n+1}$

Pf: Take $x \in M_{n+1} \subseteq M_{n+1} + N = M_n + N$

$\Rightarrow x = m_n + n'$ $\Rightarrow n' = x - m_n \in N \cap M_{n+1} = N \cap M_n$

$\Rightarrow x = m_n + n' \in M_n$.

Cor: If $M_1, \ldots, M_n$ noe, then $\bigoplus_{k=1}^{n} M_k$ noe.

Induction: $N = \bigoplus_{1}^{n-1} M_k$, $M/N = M_n$.

Cor: If R noe, then R-module M noe $\Leftrightarrow M$ fg.

Pf: "⇒" by lemma.

"⇐" Say M f.g. $M = Rx_1 + \cdots + Rx_n$.

$\bigoplus R_i \longrightarrow M$ R-linear

$(r_i) \longrightarrow \sum r_i x_i$

noe by cor. $M \cong \bigoplus R/\ker$ noe.

From now on, all rings commutative.

Thm: (Hilbert's basis thm)

If R is noe, then $R[x]$ noe.

Lemma: R noe, $I \lhd R$ noe $\Rightarrow R/I$ noe ring.

Pf: need Acc for ideals in R/I.

$\{$Ideals in $R/I\} \Leftrightarrow \{$Ideals containing $I\}$.

$\bar{I}_1 \subseteq \bar{I}_2 \subseteq \cdots\cdots \Leftrightarrow I_1 \subseteq I_2 \subseteq \cdots$

Acc $\in$ Acc

Cor: If R noe, so is $R[x_1, \cdots, x_n]/I$.

Eg: $\mathbb{Z}[i] = \mathbb{Z}[x]/x^2+1$ noe.

Pf: Say $J \lhd R[x]$, want: J f.g.

If not, pick $f_n \in J$ s.t.

f_0 = an element with smallest degree in J

$f_1 = \cdots\cdots\cdots\cdots\cdots\cdots J \setminus (f_0)$

$\vdots$

Note: $\deg f_0 \le \deg f_1 \le \cdots$

Let a_N = leading coef of $f_N \in R$.

As R noe, $(a_0) \le (a_0, a_1) \le \cdots \xrightarrow{\text{Stablizes.}} = (a_0, \cdots, a_{N-1})$

$\Rightarrow a_N = \sum \lambda_i a_i$

Take $g := \sum \lambda_i (x^{\deg f_N - \deg f_i}) f_i$

$= a_N x^{\deg f_N} + \cdots \in (f_1, \cdots, f_{N-1})$

By construction. $f_N \notin (f_1, \cdots, f_{N-1})$

But $f_N - g \notin (f_1, \cdots, f_{N-1})$. Contradiction by degree reason.

Goal: "Weak Nss": If $k = \bar{k}$, then

$$\{\text{max ideals of } k[x_1, \cdots, x_n]\} = \{(x_1 - a_1, \cdots, x_n - a_n), a_i \in k\}.$$

Def: We say a ring extension is a subring $R \subseteq S$

$\Rightarrow S$ a R-module.

$R \subseteq S$ is (module-) finite if S is a fg. R-module (finite field ext^r)

$R \subseteq S$ is finite type if $S = R[s_1, \cdots, s_n]$, some $s_i \in S$.

$R \subseteq S$ is integral if $\forall s \in S$, s satisfies $\underset{\text{monic}}{s^n} + r_{n-1}s^{n-1} + \cdots + r_0 = 0$. (Algebraic)

Ex: • $R[x]$ is fit, but not finite.

• $\mathbb{Z} \subseteq \mathbb{Q}$ not fit (denominators)

• fit $\Leftarrow$ finite.

• $\mathbb{Z} \subseteq \mathbb{Z}[i]$ integral and finite.

Lemma: Given $R \subseteq S$, TFAE for $s \in S$

① s is integral

② $R[s]$ ($\subseteq S$) is a fg. R-module

③ $\exists$ subring $R[s] \subseteq R' \subseteq S$ s.t. R' fg. R-module.

Pf: ① ⇒ ② $= s^n + r_{n-1}s^{n-1} + \cdots + r_0 = 0$

$\Rightarrow R[s] = R + Rs + \cdots + Rs^{n-1}$

② ⇒ ③ : Let $R' = R[s]$.

③ ⇒ ① : $R[s] \subseteq R' \subseteq S$. $R' = R\alpha_1 + \cdots + R\alpha_n$ fg.

$s \in R' \Rightarrow s\alpha_i \in R' \Rightarrow s\alpha_i = \sum_{j=1}^{n} r_{ij}\alpha_j$

$\Rightarrow (sI - A)\begin{pmatrix}\alpha_1 \\ \vdots \\ \alpha_n\end{pmatrix} = 0$ where $A = (r_{ij}) \in M_{n\times n}(R)$

Cor: For $R \subseteq S$ ring ext^n,

finite ⇔ fg + integral

Pf: "⇒" finite ⇒ fg. (above)

finite ⇒ integral by ③ ⇒ ①

"⇐" Say $S = R[s_1, \cdots, s_n]$, each s_i integral

$R \subseteq R[s_1] \subseteq R[s_1, s_2] \subseteq \cdots \subseteq R[s_1, \cdots, s_n]$

each "$\subseteq$" is fg by "① ⇒ ②"

$\Rightarrow R \subseteq R[s_1, \cdots, s_n]$ finite as in the proof of tower law.

Remark: $S = R[s_1, \cdots s_n]$, each s_i integral ⇒ $R \subseteq S$ finite.

Cor: Given $R \subseteq S$, then

$\tilde{R} := \{s \in S \mid s$ integral over $S\}$ form a subring.

Pf: If $s_1, s_2 \in \tilde{R}$, ⇒ $R[s_1, s_2]$ is fg R-module.

⇒ $R \subseteq R[s_1, s_2]$ finite ⇒ integral

$\Rightarrow s_1 \pm s_2,\ s_1 s_2 \in \tilde{R}$.

Lemma: If R is an UFD, $K := \mathrm{Frac} R$, then $\tilde{R} = R$

Pf: Suppose $\alpha \in K$ integral, $\alpha = \frac{a}{b}$, WLOG, $\gcd(a,b) = 1$

if $\frac{a}{b} \notin R$, $\exists$ prime π, $\pi \mid b$, $\pi \nmid a$.

As $\frac{a}{b} \in \tilde{R}$, $\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1\left(\frac{a}{b}\right) + c_0 = 0$

$\Rightarrow a^n + c_{n-1}a^{n-1}b + \cdots + c_1 a b^{n-1} + c_0 b^n = 0$

$\pi \nmid$ (first term) $\quad \pi \mid$ (remaining terms)

Contradiction.

Thm: (Zariski's lemma)

If K/k field extension of finite type,

then K/k finite.

Pf: $K = k[\alpha_1, \cdots, \alpha_n]$ by induction

$n = 1$: $K = k[\alpha_1] \Rightarrow \alpha_1$ alg. $\Rightarrow K/k$ finite.

Induction Step: $k \subseteq k(\alpha_1) \subseteq K = k[\alpha_1, \cdots, \alpha_n] = k(\alpha_1)[\alpha_2, \cdots, \alpha_n]$ (finite by induction)

If α_1 alg/k, everything is finite.

If α_1 transcendental, let $R := k[\alpha_1]$ ($\cong k[x]$) UFD,

$\forall \alpha_i$, α_i alg. over $k(\alpha_1)$

So $\alpha_i^n + \frac{r_{n-1}}{r}\alpha_i^{n-1} + \frac{r_{n-2}}{r}\alpha_i^{n-2} + \cdots + \frac{r_0}{r} = 0$ WLOG, r independent of i.

$\Rightarrow (r\alpha_i)^n + r_{n-1}(r\alpha_i)^{n-1} + \cdots + r_0 r^n = 0 \Rightarrow r\alpha_i$ integral.

Claim: $\forall \gamma \in K$, $\exists N \gg 0$, s.t. $r^N \gamma$ is integral / R

By assumption, $\gamma \in k[\alpha_1, \cdots, \alpha_n]$

$\Rightarrow r^N \gamma \in k[\alpha_1, r\alpha_2, \cdots, r\alpha_n]$

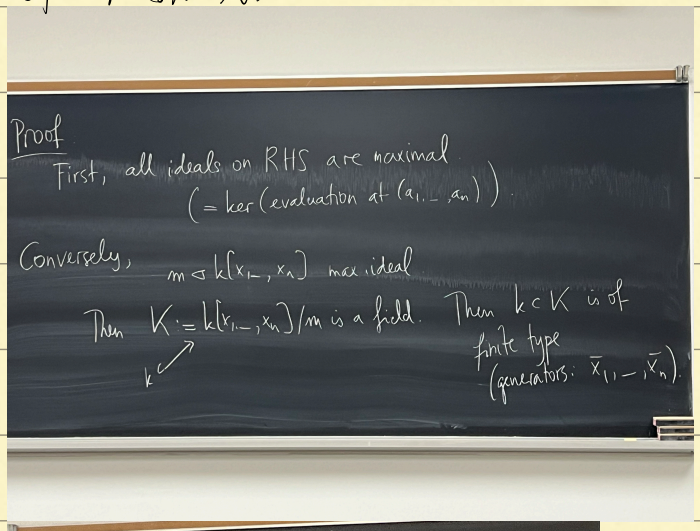
$= R[r\alpha_2, \cdots, r\alpha_n]$. integral over R.

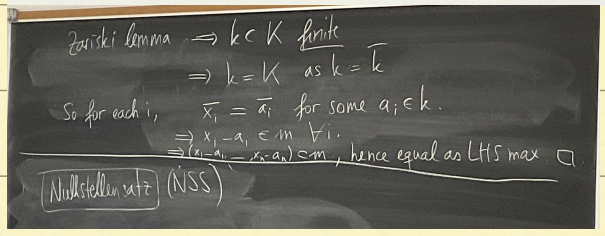
Take now $\gamma \in k(\alpha_1) = \mathrm{Frac}(R)$

claim $\Rightarrow r^N \gamma$ is int / R $\overset{\text{Lemma}}{\underset{\text{UFD}}{\Rightarrow}}$ $r^N \gamma \in R$.

Contradiction to the fact that α_i transcedental.

Pf of weak NSS





Nullstellensatz:

$$\left\{ \begin{matrix} \text{Ideals of} \\ k[x_1, \dots, x_n] \end{matrix} \right\} \underset{I}{\overset{V}{\rightleftarrows}} \left\{ \begin{matrix} \text{subsets} \\ \text{of } k^N \end{matrix} \right\}$$

$$J \longmapsto V(J) = \{ a \in k^N \mid f(a) = 0, \ \forall a \in J \}$$

$$I(X) = \{ f \mid f(a) = 0 \ \forall a \in X \} \longmapsto X$$

Def: A subset of k^n of the form $V(I)$ is called an algebraic subset

Remark: Any ideal of $k[x]$ is fg (Noe)

$\Rightarrow$ any alg. subset is zero locus? of finitely many polys

Ex: $n=1$. $k[x]$ PID

$V(f) = \{ a \in k, f(a) = 0 \}$ = finite (if $f \neq 0$)

$n=2$: $I = (y^2 - x^3 + x)$

$I = (xy)$ ⊢

Basic Properties:

(1) V, I are order reversing

(2) $V(I(X)) \supseteq X$, $I(V(J)) \supseteq J$ $\Rightarrow$ $I(V(I(X))) = I(X)$, $V(I(V(J))) = V(J)$

So V, I induces bijections between $\mathrm{Im}(I)$, $\mathrm{Im}(V)$

Thm (NSS): (1) $V(J) = \emptyset \iff J = (1)$

(2) $I(V(J)) = \sqrt{J} = \{f \mid f^N \in J, \text{ some } N \geq 1\}$

Pf: (1) = "$\in$" obvious

"$\Rightarrow$" Say $V(J) = \emptyset$, $J \neq (1)$

Choose maximal ideal $J \subseteq m = (x_1 - a_1, \cdots, x_n - a_n)$

By weak NSS, $V(J) \supseteq V(m) \neq \emptyset$

(2) = $I(V(J)) \supseteq \sqrt{J}$ = If $f^N \in J$, if $a \in V(J) \Rightarrow f^N(a) = 0 \Rightarrow f(a) = 0$

$I(V(J)) \subseteq \sqrt{J}$ = Take $f \in I(V(J))$

Reduce to (1) by Rabinowitsch trick:

Let $\tilde{J} = (J, yf - 1) \triangleleft k[x_1, \cdots, x_n, y]$

Claim: $V(\tilde{J}) = \emptyset$ =

Say $(a_1, \cdots, a_n, b) \in V(\tilde{J})$, so $(a_1, \cdots, a_n) \in V(J)$

$bf(a_1, \cdots, a_n) - 1 = 0$

But $f(a_1, \cdots, a_n) = 0$ as $f \in I(V(J))$. So $V(\tilde{J}) = \emptyset$.

By (1) = $\tilde{J} = k[x_1, \cdots, x_n, y]$

So $1 \in \tilde{J}$.

i.e. $1 = \sum_{i=1}^{s} p_i(x_1, \cdots, x_n, y) \cdot g_i(x_1, \cdots, x_n) + p(x_1, \cdots, x_n, y)\left(yf(x_1, \cdots, x_n) - 1\right)$

Evaluate f at $\frac{1}{f}$ inside $\mathrm{Frac}(k[x_1,\dots,x_n])$

$\Rightarrow 1 = \sum_i p_i(x, \frac{1}{f}) \cdot g_i(x)$

$\Rightarrow f^N = \sum_i \underbrace{f^N p_i}_{\in k[x]} \cdot g_i(x)$ as N large enough

Def: An ideal I is radical if $I = \sqrt{I}$

Remark:
- primes are radical, converse not true.

  $(x) \cap (y) = (xy) \lhd k[x,y]$.
- $\sqrt{J}$ is radical.

Cor: I, V induce order-reversing bijections between radical ideals and algebraic subsets.

Lemma: $\sqrt{I} = \bigcap_{P \supseteq I}^{\text{prime}} P$ in any comm. ring

Pf: Reduce to $I = 0$.

$R \iff R/I$

$\sqrt{I} \iff \sqrt{0}$

$P \supseteq I \iff \bar{P}$ prime

So WTS $\sqrt{(0)} = \cap p$ in R.

"$\subseteq$" if $a^n = 0$, then $a^n \in p \Rightarrow a \in p$ $\forall p$ prime.

"$\supseteq$" By contradiction, say $a \in R$, $a^n \neq 0$, $\forall n > 0$

ETS $\exists p$, s.t. $p \cap \{1, a, a^2, \dots\} = \emptyset$

Zorn: $X := \{I \lhd R,\ I \cap \{1, a, a^2, \dots\} = \emptyset\} \neq \emptyset$ as $(0) \in X$

If I_α is a chain in X, let $I = \cup_\alpha I_\alpha$ an ideal.

If $a^n \in I \Rightarrow a^n \in I_\alpha \Rightarrow \in$

So $I \in X$ upper bound.

By Zorn, $\exists J \in X$ maximal

Claim: J prime. By contradiction, if $f \notin J$, $g \notin J$, $fg \in J$.

$J \subsetneq J + (f) \ni a^n$

$J + (g) \ni a^m$

$\Rightarrow (J + (f))(J + (g)) \ni a^{m+n}$

$\Rightarrow = J + (fg) = J$ as $fg \in J$. contradiction.

(Zariski's)

Lemma: There is topology on k^n whose closed subsets are alg. subsets.

Pf: $k^n = V(1)$, $\emptyset = V(1)$

$\bigcap V(I_\alpha) = V(\sum_\alpha I_\alpha)$

Claim: $V(I) \cup V(J) = V(I \cap J)$ $(= V(IJ))$

"$\subseteq$" is clear as V order reversing.

"$\supseteq$": If $a \in V(IJ)$, but $a \in V(I)$, $a \notin V(J)$

$\Rightarrow f(a) \neq 0$ some $f \in I$, $g(a) \neq 0$ some $g \in J$.

$\Rightarrow (fg)(a) \neq 0$ and $fg \in IJ$

Remark: • $I(\cup X_\alpha) = \cap I(X_\alpha)$

• It's a very coarse topology, $n \geq 1$ not T_2

$n = 1$: "finite complement top"

Def: for $f \in k[x]$, let $D(f) = k^n \setminus V(f) = \{a \mid f(a) \neq 0\}$, open

Lemma: 1) Points of k^n are closed.

2) $D(f)$ form a basis

3) k^n is compact

4) k^n is a noetherian top. space. i.e. $\begin{cases} \text{DCC on closed subsets} \\ \text{ACC on open subsets} \end{cases}$

Pf: 1) $a \in k^n$, $\{a\} = V(x_1 - a_1, \cdots, x_n - a_n)$

2) Say $a \in \bigcup_{\text{open}} \subseteq k^n$

Write $U = k^n \setminus V(I)$ (as U open)

$\Rightarrow f(a) \neq 0$ for some $f \in I$, so $V(I) \subseteq V(f)$

$\Leftrightarrow D(f) \subseteq U$ (complement)

3) Say $k^n = \bigcup_\alpha V_\alpha$, V_α open.

By 2), write each V_α as union of $D(f)$'s, so WLOG $V_\alpha = D(f_\alpha)$

$\Rightarrow k^n = \bigcup_\alpha D(f_\alpha)$

$\Leftrightarrow \emptyset = \bigcap_\alpha V(f_\alpha) = V(\Sigma (f_\alpha))$

$\overset{\text{weak Nss}}{\Leftrightarrow} 1 \in (f_\alpha : \alpha \in A)$ ideal

$\Rightarrow 1 \in (f_{\alpha_1}, \cdots, f_{\alpha_n})$, some $\alpha_i \in A$

$\Leftrightarrow k^n = D(f_{\alpha_1}) \cup \cdots \cup D(f_{\alpha_n})$

4) Say $X_1 \supsetneq X_2 \supsetneq \cdots$ closed

$\Rightarrow I(X_1) \subsetneq I(X_2) \subsetneq \cdots \lhd k[x]$, contradiction ($k[x]$ noe)

Remark: Any algebraic subset $X \subseteq k^n$ inherits a Zariski's top.

Cor: If $X \subseteq k^n$ is a subset, then the Z. top satisfies (1) – (4)

Pf: point in $X \subseteq k^n$ closed.

Suppose $V \subseteq k^n$ alg. subset, $k[V] := k[x]/I(V)$ a reduced ring as $I(V)$ radical.

The ring homo $k[x] \longrightarrow \{\text{fns } V \to k\} \supseteq k[V] = \text{image}$.

$f(x) \longmapsto (a \mapsto f(a))$

By above, NSS induce inverse bijections

$\{\text{closed subsets of } V\} \longleftrightarrow \{\text{radical ideals of } k[V]\}$.

Def: A top. space is irreducible if

① $X \neq \emptyset$

② $X = X_1 \cup X_2$, X_i closed $\Rightarrow X_1 = X$ or $X_2 = X$

Ex: $V(X_1X_2) = V(X_1) \cup V(X_2) \subset k^2$ not irr

$k = k'$ irr as closed sets are finite

Remark: • ② $\overset{\text{complement}}{\Longleftrightarrow}$ ($\emptyset = U_1 \cap U_2 \overset{\text{open}}{\Rightarrow} U_1 = \emptyset$ or $U_2 = \emptyset$)

$\Leftrightarrow$ any 2 non-empty open sets intersects.

$\Leftrightarrow$ any nonempty open is dense.

• irred $\Rightarrow$ connected.

Prop: algebraic V is irr $\Leftrightarrow$ $I(V)$ is prime ideal

Pf: "$\Leftarrow$": If V reducible, $V = V_1 \cup V_2$ closed,

$\Rightarrow I(V) = I(V_1) \cap I(V_2)$, $I(V_i) \supsetneq I(V)$ (order-reversing)

Take $f_i \in I(V_i) \setminus I(V)$

$\Rightarrow f_1 f_2 \in I(V_1) \cap I(V_2) = I(V)$ not prime.

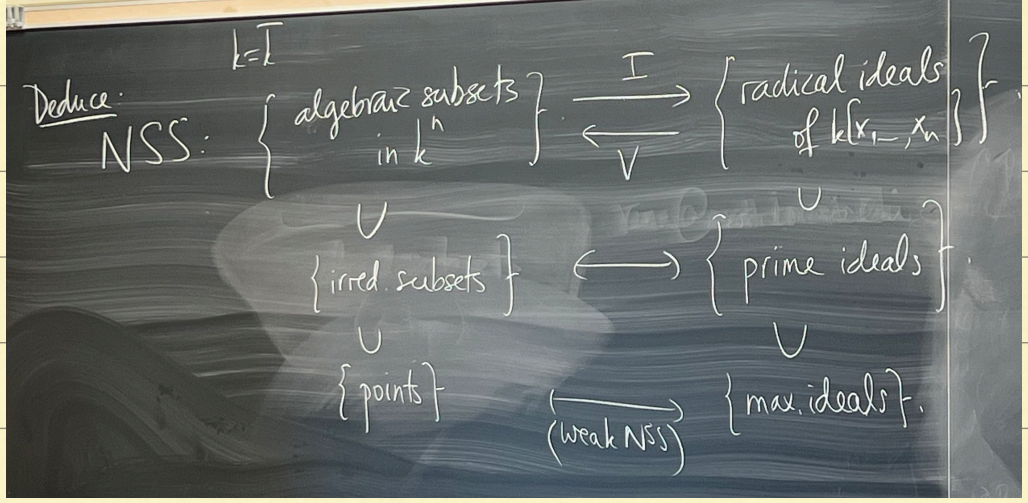
"$\Rightarrow$" If $I(V)$ not prime, take $f_1 f_2 \notin I(V)$, $f_1 f_2 \in I(V)$

Take $V_i := V \cap V(f_i)$

$V_i \subsetneq V$ as $f_i \notin I(V)$

$V_1 \cup V_2 = V \cap (V(f_1) \cup V(f_2))$ $\quad V(I) \cap V(J) = V(I \cap J) = V(IJ)$

$= V \cap (V((f_1 f_2)))$



Prop: X noetherian top. space.

Then $\exists\, X = X_1 \cup X_2 \cup \cdots \cup X_n$, X_i irre. closed. *

If $\forall i,j$, $X_i \not\subseteq X_j$, then this is unique up to ordering.

Pf: Existence: If not, X cannot be irred

$X = X_1 \cup X_1'$ proper closed.

either X_1 or X_1' doesn't have *, say X_1

$\Rightarrow X_1 = X_2 \cup X_2'$

So $X \supsetneq X_1 \supsetneq X_2 \supsetneq \cdots$, contradicts DCC on closed subsets.

Uniqueness: Write $X = X_1 \cup \cdots \cup X_n$.

Claim: $\{X_1, \cdots, X_n\} = \{\text{maximal irre. subsets of } X\}$.

Pf: If $Y \overset{\text{irred}}{\subseteq} X$, then $Y \subseteq X_1 \cup \cdots \cup X_n$

$\Rightarrow Y = (Y \cap X_1) \cup \cdots \cup (Y \cap X_n)$ (closed in Y)

$\overset{Y \text{ irred}}{\Rightarrow} Y = Y \cap X_i \Rightarrow Y \subseteq X_i$

So if $Y \subseteq X$ is any maximal irred subset,

$\Rightarrow Y \subseteq X_i \Rightarrow Y = X_i$

Conversely, each X_i max. irred.

As $X_i \subseteq Y$ irred. by *, $Y \subseteq X_j$ for some j

$\Rightarrow X_i \subseteq X_j \Rightarrow Y = X_i$

Def: The max irred subsets are called irred components of X

Remark: $\overset{\text{irred}}{Y} \subseteq X \Rightarrow \bar{Y}$ is irred.

One small application to ring theory:

Prop: Suppose $V \subseteq k^n$ alg. subset. Then $k[V] (= k[x]/I(V))$ has finitely many minimal prime ideals.

Pf: By NSS, minimal prime ideals $\Leftrightarrow$ maximal irred closed subsets of V

$=$ irred components of V.

Def: The (Jacobson) radical of a ring A is:

$$\operatorname{rad} A = \bigcap_{\substack{m \subseteq A \\ \text{maximal}}} m$$

Lemma: $x \in \operatorname{rad} A \Leftrightarrow 1 - xy \in A^\times \ \forall y \in A$

Nakayama's Lemma: M fg A module.

$I \subseteq \operatorname{rad} A$, $M = IM \Leftrightarrow M = 0$

Remark: Most general app: A is local (i.e. unique maximal ideal)

Corl: M fg A-mod. $I \subseteq \operatorname{rad} A$ $N \subseteq M$.

Then $N = M \Leftrightarrow N + IM = M$

Pf: Apply NAK to $\bar{M} = M/N = 0 \Leftrightarrow M = N$.

$I\bar{M} = \bar{M} \Leftrightarrow IM + N/N = M/N \Leftrightarrow IM + N = M$.

Cor 2: M fg A-mod, $I \subseteq \mathrm{rad}A$

Then $x_1 \cdots x_n \in M$ generate M as A-module

$\Leftrightarrow$ $\bar{x}_1 \cdots \bar{x}_n \in M/IM$ generate M/IM as A-module

Pf: Cor 1 with $N = Ax_1 + \cdots + Ax_n$

$\Leftrightarrow (N + IM = M)$

Pf 1: Let $M = Ax_1 + \cdots + Ax_n$. Assume $M = IM$

$\Rightarrow x_i = \sum_{j=1}^{n} b_{ij} x_j$, $b_{ij} \in I$.

$\Leftrightarrow (I_n - B)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$, $B = (b_{ij}) \in M_n(A)$

$\Rightarrow \mathrm{adj}(I_n - B)(I_n - B)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$.

$\Rightarrow \det(I_n - B) \cdot I_n \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$.

So $\delta = \det(I_n - B)$ kills $\forall m \in M$

$I_n - B = \begin{pmatrix} 1-b_{11} & & b_{ij} \\ & 1-b_{22} & \\ b_{ij} & & \ddots \\ & & & 1-b_{nn} \end{pmatrix} \Rightarrow \delta \in 1 + I$.

By lemma, $I \subseteq \mathrm{rad}A \Rightarrow 1 + I \subseteq A^\times \Rightarrow M = 0$.

Pf 2: Say $x_1, \cdots, x_n$ generate M, n minimal

If $M = IM$, $n \geq 1$ $(M \neq 0)$

$x_n = c_1 x_1 + \cdots + c_n x_n$

$\Rightarrow (1 - c_n) x_n = c_1 x_1 + \cdots + c_{n-1} x_{n-1}$

$1 - c_n \in 1 + I \subseteq A^*$

$\Rightarrow x_n \in \mathrm{span}(x_1, \cdots, x_n)$, contradiction

Remark: Pf 1 showed more precise result

$\forall I$, $M = IM \Rightarrow \delta M = 0$ for some $\delta \in 1 + I$

Semisimple rings / modules

Motivation: G finite group, want to study representation of G. / k.

A <u>rep. of G</u> is a k-vector space V + action $G \times V \to V$. s.t.

$V \to V$
$x \to gx$ k-linear, $\forall g \in G$.

<u>Recall</u>: $k[G]$ (group ring) $:= \{\sum_{g \in G} \lambda_g \cdot g : \lambda_g \in k\}$. $(\sum \lambda_g g)(\sum_{u,v} h) = (\sum_{g,u} \lambda_g \mu_u (gh))$

If V a representation, it becomes a $k[G]$-module.

define $(\sum \lambda_g g)(x) = \sum \lambda_g (gx)$ (using the $k[G]$-action), $\forall x \in V$.

Conversely, every $k[G]$-module arises this way.

$g \cdot x := \underset{k[G]}{g} x$

<u>Prove later</u>: if $\mathrm{char} k = 0$, every $k[G]$-module is a direct sum of simple $k[G]$-modules.

R- ring, not commutative.

M- R-module (always left)

<u>Def</u>: M is simple if $(0) \neq M$ is the only submodule.

e.g. $A = \mathbb{Z}$, $M = \mathbb{Z}/p\mathbb{Z}$.

<u>Lemma</u>: M simple $\Leftrightarrow M \cong R/m$, m maximal left ideal.

<u>Pf</u>: "$\Leftarrow$" = corresponding theorem.

"$\Rightarrow$": M simple $\Rightarrow \neq 0$. So $\exists x \in M \setminus \{0\}$.

$\lambda \mapsto \lambda x$

Then $\varphi: R \to M$, $\mathrm{im}(\varphi) = M$ as M simple.

So $M \cong R/\ker(\varphi)$, $\ker(\varphi)$ maximal by corresponding theorem.

Def: M, N R-module. Let $\mathrm{Hom}_R(M,N) = \{f : M \to N, R\text{-linear}\}$. abe group.

$\mathrm{End}_R(M) := \mathrm{Hom}_R(M,M)$ a ring

Prop: (Schur's lemma)

M, N simple module. Any $M \to N$ (R-linear) is either 0 or isom.

Cor: If $M \not\cong N$, then $\mathrm{Hom}_R(M,N) = 0$

Also, $\mathrm{End}_R(M)$ is a division ring.

e.g. • $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$

• $R = k[x]$, $M = k[x]/(f(x))$ not irred $\quad \mathrm{End}_{k[x]}(M) = k[x]/(f(x))$

• $R = D$ division ring $\quad M = D$, $\mathrm{End}_D(D) = D^{op}$ (opposite ring)

Pf: $\varphi : M \to N$

If $\ker = M$ or $\mathrm{im} = 0$ then $\varphi = 0$

otherwise, $\ker = 0$, $\mathrm{im} = N$ the φ isom.

$\mathrm{Hom}_R(\oplus M_i, N) = \oplus \mathrm{Hom}_R(M_i, N)$

$f \mapsto (f|_{M_i})$ universal property

Similar for N.

Prop: ① Suppose $M = S_1^{\oplus n_1} \oplus \cdots \oplus S_l^{\oplus n_l}$ $\quad (S^{\oplus N} = \underbrace{S \oplus \cdots \oplus S}_{N})$

S_i simple, $S_i \not\cong S_j$

then $\mathrm{End}_R(M) \cong \mathrm{End}_R(S_1^{\oplus n_1}) \times \cdots \times \mathrm{End}_R(S_l^{\oplus n_l})$ as rings

② If S simple, $D := \mathrm{End}_R(S)$

then $\mathrm{End}_R(S^{\oplus n}) \cong M_n(D)$ as rings.

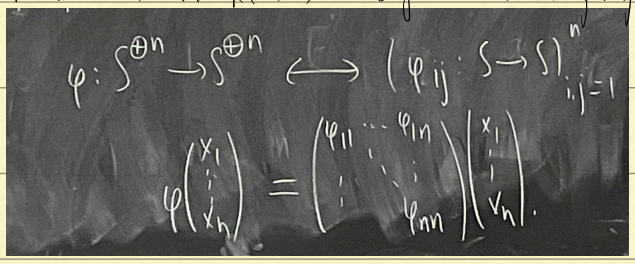
Pf: ① Claim $\varphi: M \to M \iff (\varphi_i: S_i^{\oplus n_i} \to S_i^{\oplus n_i})_{i=1}^{l}$

$\varphi(x_1, \cdots, x_l) = (\varphi_1(x_1), \cdots, \varphi_l(x_l))$

claim ⇒ ①. NTS claim.

$\mathrm{End}(\oplus S_i^{\oplus n_i}) = \mathrm{Hom}(\oplus S_i^{\oplus n_i}, \oplus S_i^{\oplus n_i}) = \oplus \mathrm{Hom}(S_i^{\oplus n_i}, S_i^{\oplus n_i})$ 交叉项是 0

② $\mathrm{End}_R(S^{\oplus n}) = \mathrm{Hom}_R(S,S)^{n^2}$ by universal property



Def: M is semi-simple if it's isomorphism to a direct sum of simple modules.

⇔ Internal direct sum of simple submodules

e.g. Any k-vector space is semi-simple.

Lemma: TFAE:

① $M = \bigoplus_{i \in I} S_i$ semisimple.

② $M = \sum_{i \in I} S_i$ (S_i simple submodule. smallest submodule containing all S_i)

③ $\forall N \overset{\text{sbmd}}{\leq} M$, $\exists N' \leq M$. s.t. $M = N \oplus N'$

Pf: ① ⇒ ② = obvious

② ⇒ ③ = Take $N \leq M$. want N'

By standard Zorn, $\exists N' \leq M$ maximal s.t. $N \cap N' = (0)$

if $N + N' = M$, done.

if not, $N + N' \subsetneq M$. By ②, $S_i \not\subseteq N + N'$ for some i.

As $(N+N') \cap S_i \subsetneq S_i$, S_i simple ⇒ $(N+N') \cap S_i = 0$

$\Rightarrow (S_i + N') \cap N \subseteq N \cap N' = 0$. Contradicts to maximality.

③$\Rightarrow$①: By Zorn, $\exists$ maximal collection S_i of simple submodules s.t. $\bigoplus_{i\in I} S_i \xrightarrow{\psi} M$ injective.

Let $N = \mathrm{im}(\psi)$. By ③, $\exists N' \subseteq M$, s.t. $M = N \oplus N'$ $\Rightarrow \in$

N' is $N' = 0$. If not, N' is $\exists S' \subseteq N'$ simple.

This is easy if $R = k[G]$ (Let $x \neq 0$ in N', then Rx contains a simple submodule by dim reason).

Cor: If M semi-simple, then so is any submodule / quotient.

If M_i semi-simple $\Rightarrow \oplus M_i$ semi-simple.

Pf: Quotient: if $\psi: M \twoheadrightarrow N$, $M = \sum S_i \Rightarrow N = \psi(M) = \sum \psi(S_i)$ ($\psi(S_i)$ is simple or 0)

$\Rightarrow N$ is semi-simple by ①

Sub: If $N \subseteq M$, then $M = N \oplus N' \Rightarrow N = M/N'$

Def: The ring is semi-simple if R is semi-simple as (left) R-module.

Prop: R semi-simple $\Leftrightarrow$ all R-module semi-simple.

Pf: "$\Leftarrow$" obvious

"$\Rightarrow$" If M is any R-module, by universal property of $\oplus$,

$\psi = \bigoplus_{m\in M} R \to M$

$(r_m) \mapsto \sum r_m \cdot m$

By Cor, $\oplus R$ semi-simple $\Rightarrow$ its quotient M is s-s

Lemma: If R ss. then $R = I_1 \oplus \cdots \oplus I_n$ for some simple

submodule (minimal ideal)

Pf: R ss $\Rightarrow R=\bigoplus_{\alpha\in A} I_\alpha$ I_α simple sbmd.

$\Rightarrow 1\in I_{\alpha_1}+\cdots+I_{\alpha_n}$, some distinct $\alpha_1,\cdots,\alpha_n\in A$

$\Rightarrow R\in RI_{\alpha_1}+\cdots+RI_{\alpha_n}=I_{\alpha_1}+\cdots+I_{\alpha_n}\leq R$

$\Rightarrow R=I_{\alpha_1}\oplus\cdots\oplus I_{\alpha_n}$ ∎

Cor: If R semi-simple, $R=I_1\oplus\cdots\oplus I_n$, then any simple R-module is isom to I_j for some j

Pf: If S simple, let $x\in S\setminus\{0\}$, $\varphi: R\xrightarrow{r\mapsto rx} S$. $\exists I_j$, $\varphi|_{I_j}\neq 0$.

So $\varphi|_{I_j}: I_j\to S$ isom by Schur.

Def: R ring, R^{op} = opposite ring, $R=R^{op}$ as abelian group,

R^{op}: $y*x=xy$ (R: xy)

Remark: $M_n(R)^{op}\cong M_n(R^{op})$

$A\mapsto A^T$

Lemma: If R is a ring, then

$R^{op}\cong End_R(R)$ As an R-module.

$r\mapsto(\varphi_r: x\to xr)$

Pf: • $\varphi_r: R\to R$ is R-linear. $(\lambda x+y)r=\lambda(xr)+yr$.

• φ is a ring-homo. $\varphi(1)=\varphi_1=id$

$\varphi_{r+s}=\varphi_r+\varphi_s$ $\quad x(r+s)=xr+xs$ ✓

$\varphi_{r*s}=\varphi_r\circ\varphi_s$ $\quad x(r*s)=\overset{x(sr)}{\overset{\shortparallel}{(xs)}}r$ ✓

• injective: If $\varphi_r=0$, $\overset{r}{\overset{\shortparallel}{\varphi_r(1)}}=0$

• surjective: $\psi: R \to R$. then $\psi(r) = r\psi(1) \Rightarrow \psi = \psi_{\psi(1)}$

Thm: (Artin-Wedderburn):

R semi-simple $\Leftrightarrow R \cong M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s)$, D_i division rings.

Pf: "$\Rightarrow$": By lemma, $R = I_1 \oplus \cdots \oplus I_N$, I_j simple.

WLOG (reordering): $I_1, \cdots, I_s$ are pairwise non-isom.

$\forall j > s$, $\exists k \le s$, s.t. $I_j \cong I_k$.

So $R \cong I_1^{\oplus n_1} \oplus \cdots \oplus I_s^{\oplus n_s}$

By lemma: $R^{op} \cong End_R(I_1^{\oplus n_1} \oplus \cdots \oplus I_s^{\oplus n_s})$ As module

$\cong M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s)$, $D_j = End_R(I_j)$ division ring.

$\Rightarrow R \cong M_{n_1}(D_1)^{op} \times \cdots \times M_{n_s}(D_s)^{op} \cong M_{n_1}(D_1^{op}) \times \cdots \times M_{n_s}(D_s^{op})$.

For converse.

Prop: Suppose $R = M_n(D)$ D division ring.

① The module $S = D^{\oplus n}$ (column vectors, under matrix multiplication)

is simple.

② $R \cong S^{\oplus n}$ as R-module. So R is a semi-simple ring

③ Any simple R-module is isom to S

Useful notation: $E_{ij} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$ (i-th row, j-th column) $\in R$

$e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ (i-th row) $\in S$. So $E_{ij} e_k = \delta_{jk} e_i$

Pf: ① $S = D^{\oplus n}$, ETS $\forall x \in S \setminus \{0\}$, $Rx = S$.

Write $x = \sum_{k=1}^{n} e_k d_k$ ($d_k \in D$), say $d_j \neq 0$

$\Rightarrow E_{ij} x = e_i d_j$ ($= d_j e_i$) $\overset{\text{division ring}}{\Rightarrow} e_i \in Rx \Rightarrow S \subseteq Rx$.

② $R = M_n(D) = I_1 \oplus \cdots \oplus I_n$, where $I_i = \{x \in M_n(D), \text{ zero outside } i\text{th column}\}$

Then $I_i \subseteq R$ is an R-submodule (i.e. left ideal)

and $S \cong I_i$, $\begin{pmatrix} d_1 \\ d_n \end{pmatrix} \Leftrightarrow (0 \cdots \overset{d_i}{d_n} \cdots 0)$

③ By some car above.

Exercise: Show R is simple ring.

Suppose A, B are rings, $R = A \times B$.

$\to e = (1,0)$, $f = (0,1)$, central. $e^2 = e$, $f^2 = f$, $ef = 0$, $e + f = 1$.

If N is any A-module, can consider it as R-module

via $R = A \times B \to A \to \mathrm{End}_{\mathbb{Z}}(N)$ (ring hom.)

If P is a B-module, consider it as another projection.

$\rightsquigarrow N \oplus P$ is R-module.

Conversely, M an R-module, $M = eM \oplus fM$

eM killed by $(0) \times B = Rf$, so is an $\frac{A \times B}{(0) \times B} \cong A$-module.

fM similarly.

Prop: ① We have "functions" (functors)

$$(A\text{-mod}) \times (B\text{-mod}) \underset{\varphi}{\overset{\psi}{\rightleftarrows}} (R\text{-module})$$

$$(N, P) \longrightarrow N \oplus P$$

$$(eM, fM) \longleftarrow M.$$

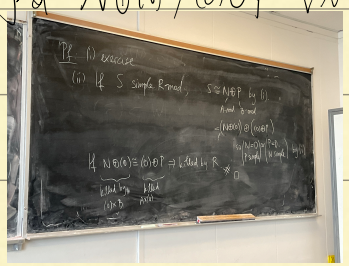
s.t. $\psi(\varphi(N,P)) \cong (N,P)$, $\varphi(\psi(M)) = M$.

(equivalence of categories)

② The simple R-module are (up to isom)

$N \oplus (0)$, $(0) \oplus P$ And $N \oplus (0) \neq (0) \oplus P$ $\forall N, \forall P$.

↑ simple A-mod ↑ simple B-mod.



Remark: If R ss, simple mod $S_1, \cdots, S_k$ (up to isom)

By construction: $D_i^{op} = \mathrm{End}_R(S_i)$

Last time: $M_n(D)$ semi-simple: only simple module $D^{\oplus n}$

Pf: "$\in$":

showed if $R = A \times B$, simple R-module are precisely

$N \oplus (0)$, $(0) \oplus P$

↑ simple A-mod ↑ simple B-mod

Cor: A, B semi-simple rings, then $A \times B$ semi-simple

Let $S_1, \cdots S_k$ simple A-mod up to isom,

$\cdots S_1' \cdots S_l' \cdots B \cdots$.

So we have $k+l$ simple R-mod, $S_i \oplus (0)$, $(0) + S_j'$

Pf: Write $A = I_1 \oplus \cdots \oplus I_r$, $B = J_1 \oplus \cdots \oplus J_s$ simple.

$\Rightarrow R = A \times B = A \oplus B = (I_1 \oplus 0) \oplus \cdots \oplus (0 \oplus J_1) \oplus \cdots$ All simple.

$\Rightarrow R$ is semi-simple R-mod, therefore s.s. ring.

Cor: If $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s)$, then

① R semi-simple ring

② R has precisely s simple module up to isom

$(0) \oplus \cdots \oplus (D_i^{\oplus n_i}) \oplus \cdots \oplus (0)$

Remark: R simi-simple $\Leftrightarrow R^{op}$ semi-simple.

Application: Let k be a field.

Def: A **k-algebra** is a ring A together with a ring homo:

$k \hookrightarrow Z(A)$ (center of A)

Eg: a) A field extension K/k

b) A division ring with center $= k$

c) $k[G]$ group ring.

d) $M_n(k)$, or $M_n(A)$ (A k-alg) $\quad k \to M_n(A)$, $\lambda \mapsto \lambda I$

e) $M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s)$ if $k \le Z(D_i)$, $\forall i$

$\lambda(xy) = (\lambda x)y = x(\lambda y)$ ($x \in Z(G)$)

Remark: Any k-alg A becomes a k-vector space.

often talk about fid. k-alg.

Cor: If R is a fid k-algebra that is semi-simple,

then $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s)$, where D_i is a fid.

division k-algebra. and $\dim_k R = \sum_{i=1}^{s} n_i^2 \dim_k D_i$

Pf: $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s)$ as ring. D_i division ring.

k-alg: ring homo $k \to Z(R) = Z(M_{n_1}(D_1)) \times \cdots \times Z(M_{n_s}(D_s)) = Z(D_1) \times \cdots \times Z(D_s)$ ($k \to (z, \ldots, z)$)

$\Leftarrow$ uni. prop $\Rightarrow$ ring homo $k \to Z(D_i)$

$\Rightarrow D_i$ k-alg.

Lemma: Let $k = \bar{k}$, D is a fid. division ring. then $D = k$

Pf: If not. pick $\delta \in D \setminus k$. then $k \subsetneq k[\delta] \subseteq D$. ($k[\delta]$: commutative subring.)

finite dim $\Rightarrow k[\delta]$ a field, contradiction.

Cor: If $k = \bar{k}$, R a fid. semi-simple k-alg.

then $R \cong M_{n_1}(k) \times \cdots \times M_{n_c}(k)$

S_i column vectors, as R-module. $R \cong S_1^{\oplus n_1} \oplus \cdots \oplus S_c^{\oplus n_c}$

• $\exists$ div. algebra / $\mathbb{C}$. that are much bigger than $\mathbb{C}$ ($\mathbb{C}(x)$)

Thm: (Maschke)

Suppose G a finite group, k any field that $|G| \in k^\times$ (if $\mathrm{char} k = p$, then $p \nmid |G|$)

Then $k[G]$ is a semi-simple ring.

Pf: NTS: if M is any $k[G]$-mod. $N \subseteq M$ submd. $\exists N'$, s.t. $M = N \oplus N'$

First, find $N' \leq M$ k-subspace s.t. $M = N \oplus N'$

$\to$ get projection map $\pi: M \to N$, k-linear and $\pi|_N = \mathrm{id}$. ($n + n' \mapsto n$)

Define $f: M \to N$

$$m \mapsto \frac{1}{|G|} \sum_{g \in G} g(\pi(g^{-1}m)) \qquad (g^{-1}m \in N)$$

Claim: f is $k[G]$-linear and $f|_N = \mathrm{id}$. ($\Rightarrow M = N \oplus \ker f$, since $m = f(m) + (m - f(m))$)

Pf: 1) f is k-linear since π is k-linear and $\lambda g = g\lambda$ $\forall \lambda \in k$, $g \in G$.

2) for $h \in G$, $f(hm) = \frac{1}{|G|} \sum_{g \in G} g(\pi(g^{-1}hm))$ $\quad g' = h^{-1}g$

$$= \frac{1}{|G|} \sum_{g \in G} hg'(\pi((g')^{-1}m))$$

$$= hf(m)$$

3) by 1) + 2), f is $k[G]$-linear.

4) for $n \in N$, $f(n) = \frac{1}{|G|} \sum_{g \in G} g(\pi(g^{-1}n)) = \frac{1}{|G|} \sum_{g \in G} g(g^{-1}n) = n$ ($g^{-1}n \in N$)

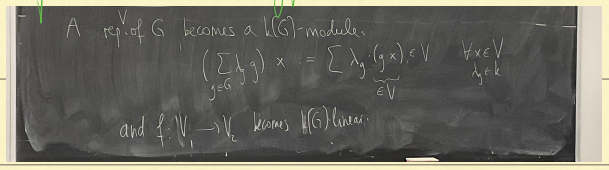
Remark: if $\mathrm{char} k = p \mid |G|$, not semi-simple.

Representations of finite groups

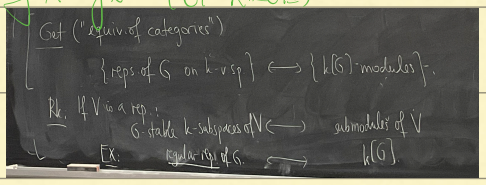
G finite group, k field.

Recall: A representation of G is a k-vector space $+$ a group action $G \times V \to V$, s.t. $V \to V$ is linear $\forall g \in G$. ($x \mapsto gx$)

- A homo $V_1 \to V_2$ of G reps. V_1, V_2 is a k-linear map $f: V_1 \to V_2$ s.t. $f(gx) = gf(x)$, $\forall x \in V_1$, $\forall g \in G$.
- rep of G $\Leftrightarrow$ gp homo $G \to GL(V)$ ($g \longmapsto (x \to gx)$)



- Conversely, if M a $k[G]$ module, can make it into G-rep $g \cdot x = gx$ ($G \subseteq k[G]$)



- Two group homos $\rho_1, \rho_2: G \to GL(V)$ on same V are isom $\Leftrightarrow$ they are conjugate by some $X \in GL(V)$ i.e. $\rho_1(g) = X \rho_2(g) X^{-1}$, $\forall g \in G$.

In particular, if $\chi_1 \neq \chi_2$ $G \to GL(V)$ then $\chi_1 \neq \chi_2$ as reps.

From now on, $k = \mathbb{C}$ (mostly works for $k = \bar{k}$, $\mathrm{char} = 0$)

And all representations are f.d.

Thm: Let $S_1, \cdots, S_r$ be irre. representations up to isom

① r = # of conj classes of G.

② for every rep. V, $V \cong S_1^{\oplus a_1} \oplus \cdots \oplus S_r^{\oplus a_r}$ with unique a_i

③ $\mathbb{C}[G] \cong \bigoplus_{i=1}^{r} S_i^{\oplus \dim_{\mathbb{C}} S_i}$

④ $|G| = \sum_{i=1}^{r} (\dim_{\mathbb{C}} S_i)^2$

Rf: S_i are the simple $\mathbb{C}[G]$-modules.

Maschke + A-W

$\Rightarrow \mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$

and semi-simple modules are $S_i = \mathbb{C}^{\oplus n_i}$ (up to isom)

Already saw ③, (③ ⇒ ④ by taking dimension)

② in HW4 Q1

① = Recall: $\underbrace{Z(\mathbb{C}[G])}_{\text{compute this}} = Z(M_{n_1}(\mathbb{C}) \times \cdots$

$= \mathbb{C} \times \mathbb{C} \times \cdots \times \mathbb{C}$ (r th)

$\sum \lambda_g \cdot g \in Z(\mathbb{C}[G])$

$\Leftrightarrow h(\sum \lambda_g \cdot g) = (\sum \lambda_g \cdot g)h$

$\Leftrightarrow \sum \lambda_g \cdot hgh^{-1} = \sum \lambda_g \cdot g$

$\Leftrightarrow \lambda_{h^{-1}gh} = \lambda_g, \ \forall g, h \in G$

$g \mapsto \lambda_g$

$\Leftrightarrow G \to \mathbb{C}$ is constant on conjugacy classes. ("class function")

$\Rightarrow Z(\mathbb{C}[G]) = \{\sum f(g)g : f = \{\text{conjugacy classes of } G\} \to \mathbb{C}\}$

$\dim$ = # conjugacy class = r as above.

Example: $G = S_3$. 3 conjugacy classes. $|1|, |2|, 3$

By Thm, 3 irre. reps.

Found: trivial, sign ($\text{odd} \to -1$, $\text{even} \to 1$) called V

Theorem ④: $|S_3| = n_1^2 + n_2^2 + n_3^2 \Rightarrow n_3 = 4$ (6)

2-dim: $S_3 \cong D_6$ acts on $\mathbb{R}^2$ (sym of $\triangle$)

Def: The character of a resp. V is the function

$\chi_V : G \to GL(V) \xrightarrow{\text{trace}} \mathbb{C}$

As $\text{tr}(ABA^{-1}) = \text{tr}(B)$, so χ_V is a class function.

$\rightsquigarrow$ notion of trivial / irred resp.

Example: $G = S_3$. find all irred. chars:

$\mathbb{1}$, sign: $S_3 \to \mathbb{C}^\times \xrightarrow{tr} \mathbb{C}$

character table:

	e	(12)	(123)
$\chi_{\mathbb{1}}$	1	1	1
χ_{sgn}	1	-1	1
χ_V	2	0	-1

$(12) \to$ reflection

$(123) \to$ rotation $\to \begin{pmatrix} e^{\frac{2\pi i}{3}} & \\ & e^{-\frac{2\pi i}{3}} \end{pmatrix}$

Lemma: If V is G-rep $\Leftrightarrow \rho_V : G \to GL(V)$

① $\chi_V(1) = \dim_{\mathbb{C}}(V)$

② $\rho_V(g)$ is diagonalizable $\forall g$

③ if $g \in G$ has order n, then $\chi_V(g)$ is a sum of $(\dim V)$ many n^{th} root of unity.

④ $|\chi_V(g)| \le \chi_V(1)$ $\forall g$

⑤ $\chi_V(g^{-1}) = \overline{\chi_V(g)}$ $\forall g$

Pf: ① obvious ($\rho_V(1) = I$)

② $g^n = 1 \Rightarrow \rho_V(g)^n = 1$ in $GL(V)$

$\Leftrightarrow$ minimal polynomial of $\rho_V(g)$ divides $x^n - 1$

Fact: $\alpha \in GL(V)$ diag $\Leftrightarrow$ its min poly has no repeated rots.

$\Rightarrow \rho_V(g)$ is diag.

G-rep ($G \times V \to V$) $\leftrightarrow$ $G \to GL(V)$

$\updownarrow$

$\mathbb{C}[G]$-module

A-W $\Rightarrow$ $\begin{cases} \#\text{ of irred-reps} = \#\text{ of conjugacy classes} \\ \mathbb{C}[G] \simeq \bigoplus_{i}^{r} S_i^{\oplus \dim_{\mathbb{C}} S_i} \\ \Rightarrow |G| = \sum (\dim_{\mathbb{C}} S_i)^2 \end{cases}$

character: $G \xrightarrow{\rho_V} GL(V)$

$\chi_V \searrow \quad \downarrow \mathrm{tr}$

$\mathbb{C}$

Pf: (cont.)

③: $g^n = 1 \Rightarrow \rho_V(g)^n = Id$

$\Rightarrow \rho_V(g) \widetilde{\text{conj}} \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_d \end{pmatrix}$, $\lambda_i^n = 1$

④: $\chi_V(g) = |\lambda_1 + \cdots + \lambda_d| \le d$

⑤: $\chi_V(g^{-1}) = \lambda_1^{-1} + \cdots + \lambda_d^{-1} = \bar{\lambda}_1 + \cdots + \bar{\lambda}_d = \overline{\chi_V(g)}$

Prop: The irred characters are linearly independent / $\mathbb{C}$

$\Rightarrow$ they form a $\mathbb{C}$-basis of class functions.

Pf: Define $\widetilde{\chi}_V : \mathbb{C}[G] \to \mathbb{C}$

$x \mapsto \mathrm{tr}(x: V \xrightarrow{V \mapsto xV} V)$ $\quad (\widetilde{\chi}_V|_G = \chi_V)$

Say $S_1, \cdots, S_r$ are the simple $\mathbb{C}[G]$-module up to isom.

If $\sum_{i=1}^{r} \lambda_i \chi_{S_i} = 0$ $(\lambda_i \in \mathbb{C})$ as $f_n\ G \to \mathbb{C}$

$\Leftrightarrow \sum_{i=1}^{r} \lambda_i \widetilde{\chi}_{S_i} = 0$ as $f_n : \mathbb{C}[G] \to \mathbb{C}$

Write $\mathbb{C}[G] \overset{\sim}{=} \prod_{i=1}^{r} M_{n_i}(\mathbb{C}) \curvearrowright \mathbb{C}^{\oplus n_i} = S_i$

take $x = (0, \cdots, \underset{j\text{-th}}{I}, \cdots, 0)$: $\sum \lambda_i \widetilde{\chi}_{S_i}(x) = 0$

($= 0$ if $j \neq i$; $= n_j$ if $j = i$)

$\Rightarrow \lambda_j n_j = 0$, so $\lambda_j = 0$, $\forall j$

Cor: ① Every character of G is uniquely of the form $\sum_{i=1}^{r} l_i \chi_i$

② $V_1 \cong V_2 \Leftrightarrow \chi_{V_1} = \chi_{V_2}$.

Def: If G acts on a finite group X, define a

permutation representation $= \mathbb{C}X := \{\sum_{x\in X} \lambda_x \cdot x : \lambda_x \in \mathbb{C}\}$

(basis given by X, $\dim = |X|$)

G-rep: $g \cdot (\sum \lambda_x x) = \sum \lambda_x \cdot gx$

Example: if $G \curvearrowright G$ by $g \cdot h = gh$, $\mathbb{C}G = \mathbb{C}[G]$.

Lemma: (permutation character)

If $G \curvearrowright X$, $\chi_{\mathbb{C}X}(g) = \#\{x \in X \mid gx = x\}$

Pf: Orbits of g: $x_1 \mapsto x_2 \mapsto \cdots \mapsto x_k$ $\quad x_{k+1} \mapsto \cdots$

In this basis, $g = \begin{pmatrix} 0 & & & 1 \\ 1 & 0 & & \\ & \ddots & & \\ & & 1 & 0 \end{pmatrix}$

So $\mathrm{tr}(g) = \#$ of 1-orbits.

Example: $\chi_{\mathbb{C}G} = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{if } g \neq 1 \end{cases}$

Other representations:

If V, W G-reps, get

$V \oplus W$: $g(v, w) = (gv, gw)$

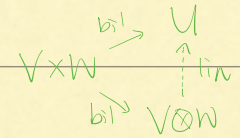
$V \otimes_{\mathbb{C}} W$ = tensor product as vector spaces

Recall: $\exists$ bilinear fn $V \times W \to V \otimes W$

$(x, y) \to x \otimes y$.

universal prop: if $V \times W \to U$ bilinear, then

$\exists!$ linear function $V \otimes W \to U$, s.t.



If $f_1: V_1 \to W_1$, $f_2: V_2 \to W_2$ linear, get

unique linear $V_1 \otimes V_2 \to W_1 \otimes W_2$

$$x \otimes y \mapsto f_1(x) \otimes f_2(y)$$

Fact: if (e_i), (f_j) basis of V, W

then $(e_i \otimes f_j)$ basis of $V \otimes W$

For $V \otimes_{\mathbb{C}} W$, $g \in G$, $V \otimes W \to V \otimes W$

$$f_V(g) \otimes f_W(g)$$

$\mathrm{Hom}_{\mathbb{C}}(V,W) := \{V \to W \mid \mathbb{C}\text{-linear}\}$

$g \in G$ acts as $\mathrm{Hom}_{\mathbb{C}}(V,W) \to \mathrm{Hom}_{\mathbb{C}}(V,W)$

$$f \mapsto f_V(g) \circ f \circ f_V(g^{-1})$$

i.e $(x \mapsto g f(g^{-1}x))$

$V^* := \mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C})$, so special case of Hom-rep

concretely, $V^* \to V^*$

$$f \mapsto (x \mapsto f(g^{-1}x))$$

Lemma: $\mathrm{Hom}_{\mathbb{C}}(V,W) \cong V^* \otimes W$ as G-rep.

Pf: By univ. prop, we have linear map

$$V^* \otimes_{\mathbb{C}} W \to \mathrm{Hom}_{\mathbb{C}}(V,W)$$

$$\theta : (f \otimes w \to (v \to f(v)w))$$

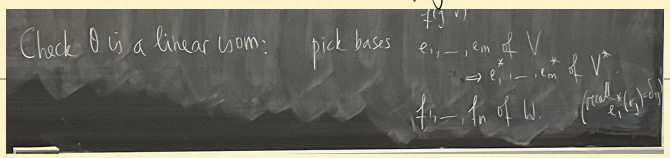
Check this is a map of G-reps

$$\begin{array}{ccc} f \otimes w & \xmapsto{\theta} & (v \mapsto f(v)w) \\ \downarrow g & & \downarrow g \end{array}$$

$g f) \otimes g w \xmapsto{\theta} v \mapsto g[f(g^{-1}v)w] = f(g^{-1}v)gw$

$(v \mapsto [(gf)(v)]gw$ //)

$f(g^{-1}v)$



$\Rightarrow e_i^* \otimes f_j$ basis of $V^* \otimes W$

$\theta(e_i^* \otimes f_j) \in \mathrm{Hom}_{\mathbb{C}}(V, W) \cong M_{n \times m}(\mathbb{C})$

sends $e_k \longmapsto e_i^*(e_k) f_j = \delta_{ik} f_j$

matrix $\begin{pmatrix} 0 & & 0 \\ & \ddots & \\ 0 & & 0 \end{pmatrix} \leftarrow j$

$\uparrow i$

Lemma: ① $\chi_{V \oplus W} = \chi_V + \chi_W$

② $\chi_{V \otimes W} = \chi_V \cdot \chi_W$

③ $\chi_{\mathrm{Hom}(V,W)} = \overline{\chi_V} \cdot \chi_W$

④ $\chi_{V^*} = \overline{\chi_V}$

Pf: ① obvious

② WTS if $f: V \to V$, $h: W \to W$ linear,

then $\mathrm{tr}(f \otimes h) = \mathrm{tr}(f)\mathrm{tr}(g)$

Pick basis (e_i) of V, (f_j) of W,

$f(e_i) = \sum_j a_{ji} e_j$

$h(f_j) = \sum_l b_{lk} f_l$

$(f \otimes h)(e_i \otimes f_k) = f(e_i) \otimes h(f_k)$

$= \underbrace{\sum_j \sum_l a_{ji} b_{lk} (e_j \otimes f_l)}$

coeff of $e_i \otimes f_k$ equals $a_{ii} b_{kk}$

So $\mathrm{tr}(f \otimes h) = \sum_i \sum_k a_{ii} b_{kk} = \mathrm{tr}(f)\mathrm{tr}(h)$

④ $g: V^* \to V^*$

$f \mapsto f \circ g^{-1}$ is the transpose map of $g^{-1}: V \to V$

So $\mathrm{tr}(g \text{ on } V^*) = \mathrm{tr}(\bar{g}^{-1} \text{ on } V)$

$\Rightarrow \chi_{V^*}(g) = \chi_V(\bar{g}^{-1}) = \overline{\chi_V(g)}$

③ $\mathrm{Hom}_{\mathbb{C}}(V, W) \cong V^* \otimes W$

so $\chi_{\mathrm{Hom}(V,W)} \overset{②}{=} \chi_{V^*}\chi_W \overset{④}{=} \overline{\chi_V}\cdot\chi_W$

Def: If $\chi, \psi : G \to \mathbb{C}$ class functions

define $\langle \chi, \psi \rangle := \frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\psi(g)} \in \mathbb{C}$ is pos. def. hermitian inner product

$= \frac{1}{|G|}\sum_{i=1}^{r} |\underbrace{cc(g_i)}_{\text{conj. class}}|\,\chi(g_i)\overline{\psi(g_i)}$

Lemma: If V is a G-rep, then

$\langle \chi_V, \mathbb{1} \rangle = \dim_{\mathbb{C}}(V^G)$, where $V^G := \{x \in V \mid x = gx, \forall g\}$

Pf: Define $\pi : V \to V^G$

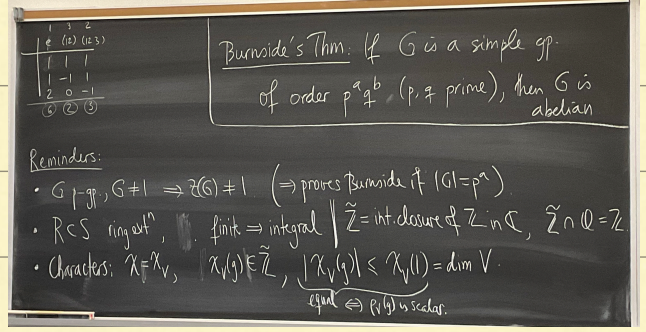
$x \longmapsto \frac{1}{|G|}\sum_{g\in G} gx$ then $\pi|_{V^G} = id. \Rightarrow \pi^2 = \pi$

$\Rightarrow V = V^G \oplus \ker(\pi)$

$x \mapsto (\underbrace{\pi(x)}_{\pi = id}, \underbrace{x - \pi(x)}_{\pi = 0})$

So $\mathrm{tr}(\pi) = \dim(V^G)$

$\| \frac{1}{|G|}\sum_{g\in G}\mathrm{tr}(\underbrace{g : V \to V}_{\chi_V(g)}) = \langle \chi_V, \mathbb{1} \rangle$



Prop: If V is an irre. rep of G, then $\dim V = \chi_V(1)$ divides $|G|$

Pf: Let $g_1, \dots, g_r$ represent the conj classes

Let $e_i = \sum_{g \in cl(g_i)} g \in Z(\mathbb{C}[G])$, even in $Z(\mathbb{Z}[G])$

Note: ring ext^n $\mathbb{Z} \subset Z(\mathbb{Z}[G])$ finite (since $\subset \mathbb{Z}[G]$, $\mathbb{Z}$ noetherian)

so integral, so e_i integral /$\mathbb{Z}$

Have ring homo: $\Psi : Z(\mathbb{C}[G]) \longrightarrow End(V) \overset{\text{schur}}{\cong} \mathbb{C}$

$$z \longmapsto (z : V \to V) = \begin{pmatrix} \psi(z) & & \\ & \ddots & \\ & & \psi(z) \end{pmatrix}$$

e_i is integral /$\mathbb{Z}$ $\Rightarrow$ $\Psi(e_i) \in \tilde{\mathbb{Z}}$

Compute $tr(e_i : V \to V) = n \cdot \Psi(e_i)$, where $n := \dim_{\mathbb{C}} V$

$$\sum_{cl(g_j)} tr(g_j) = |cl(g_j)| \chi_V(g_j)$$

$$\Rightarrow \frac{|cl(g_i)|}{n} \cdot \chi_V(g_i) \in \tilde{\mathbb{Z}}$$

$$\Rightarrow \tilde{\mathbb{Z}} \ni \sum_{i=1}^{r} \frac{|cl(g_i)|}{n} \cdot \chi_V(g_i) \overline{\chi_V(g_i)} = \frac{|G|}{n} \langle \chi_{V_i}, \chi_V \rangle \in \mathbb{Z} \Rightarrow \frac{G}{n} \in \tilde{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$$

Lemma: Suppose V is an irre. rep of $\dim n$. $C_j := |cl(g_j)|$

if $\gcd(n, C_j) = 1$, then $|\chi_V(g_j)| = 0$ or $n \ (= \chi_V(1))$

Pf: By above, $\frac{C_j}{n} \chi_V(g_j) \in \tilde{\mathbb{Z}}$, also $\chi_V(g_j) \in \tilde{\mathbb{Z}}$

as $\gcd(n, C_j) = 1$, $1 = an + bC_j \Rightarrow \frac{1}{n} \chi_V(g_j) \in \tilde{\mathbb{Z}}$ ($:= \alpha$)

Also, $|\alpha| = \frac{|\chi_V(g_j)|}{\chi_V(1)} \leq 1$

Let $N :=$ Galois closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$, $G := Gal(N/\mathbb{Q})$

$\beta := \prod_{\sigma \in G} \sigma(\alpha) \in N^G = \mathbb{Q}$, but also $\sigma(\alpha) \in \tilde{\mathbb{Z}}$, $\forall \sigma$

$\Rightarrow \beta \in \tilde{\mathbb{Z}} \Rightarrow \beta \in \mathbb{Z}$

Now, $\alpha = \frac{\chi_V(g_j)}{n} = \frac{\zeta_1 + \cdots + \zeta_n}{n}$ (ζ_i some roots of unity)

$|\sigma(\alpha)| = \left|\frac{\sigma(\zeta_1)+\cdots+\sigma(\zeta_n)}{n}\right| \leq 1$, $\forall \sigma$

$\Rightarrow |\beta| \leq 1 \overset{\beta \in \mathbb{Z}}{\Rightarrow} |\beta| = 0$ or $1 \Rightarrow |\alpha| = 0$ or 1

Thm: (Burnside) $p \neq q$ primes (Shorter: G abe)

If $|G| = p^a q^b$, then G is solvable.

Pf: Take composition series:

$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_N = G$, G_i/G_{i+1} simple.

So WLOG G simple, WTS G abelian

By construction: Assume G is non-abelian, simple. $|G| = p^a q^b$

As p-groups solvable, $a > 0$, $b > 0$.

Let $\text{Irr}(G) = \chi_1, \ldots, \chi_r$ be irre reps of G, $\chi_i = \chi_{V_i}$.

Let $Z_i = \{g \in G \mid |\chi_i(g)| = \chi_i(1)\} \Leftrightarrow \rho_{V_i}(g)$ is a scalar

so $Z_i \lhd G$

G is simple $\Rightarrow Z_i = 1$ or $Z_i = G$

If $Z_i = G$, $\Rightarrow G$ acts as scalars of $V_i \Rightarrow \dim V_i = 1$

$\rho_{V_i}: G \to \mathbb{C}^\times$, so $\ker = 1$ or G
(contradicts to G non-abe; $V_i = \mathbb{1} \Rightarrow i = 1$)

$\Rightarrow Z_i = 1$, $\forall i > 1$ *

Take $1 \subsetneq Q \subsetneq G$, a q-sylow group, $|Q| = q^b > 1$ ($\Rightarrow Z(Q) \neq 1$)

Take $h \in Z(Q) \setminus \{1\}$

$\Rightarrow C_G(h) > Q \Rightarrow (G : C_G(h)) \mid (G : Q) = p^a$

($(G : C_G(h)) = |cl(h)|$)

Recall: $\chi_i(1) \mid |G| = p^a q^b$

If $p \nmid \chi_i(1)$, then $\chi_i(1) \mid q^b$, so $\gcd(\chi_i(1), |cl(h)|) = 1$

$\overset{\text{Lemma}}{\Rightarrow} |\chi_i(h)| = 0$ or $\chi_i(1)$

in this case, $h \in \mathbb{Z}_i$

$\overset{*}{\Rightarrow} i = 1$

If $p \nmid \chi_i(1)$ and $i > 1$, then $\chi_i(h) = 0$

Column orthogonality: use $h \neq 1$:

$$0 = \sum_{i=1}^{r} \chi_i(h)\chi_i(1) = \underset{(i=1)}{1} + \sum_{p \nmid \chi_i(1)} \underbrace{\chi_i(1)}_{\in p\mathbb{Z}} \cdot \underbrace{\chi_i(h)}_{\in \hat{\mathbb{Z}}} \in p\hat{\mathbb{Z}}$$

$\Rightarrow \frac{-1}{p} \in \hat{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$, contradiction.

Restriction + induction

Suppose $H \leq G$. Then $V|_H : H \to GL(V)$ is a representation of H

Other way: If W is an H-rep, let

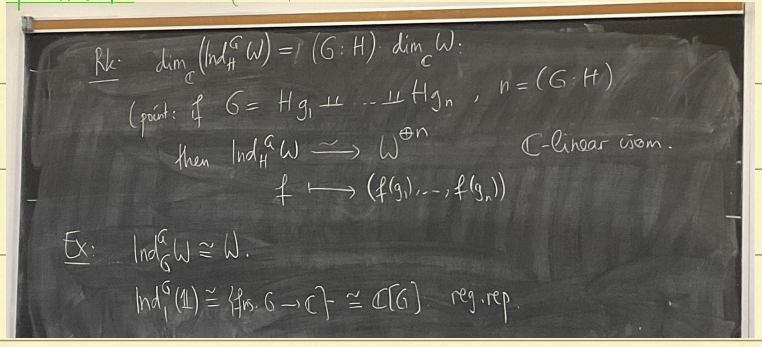
$$\mathrm{Ind}_H^G W := \{f : G \to W : f(hg) = h f(g), \ \forall h \in H, g \in G\}.$$

- $\mathbb{C}$-vector space by pointwise operations
- G-action: if $\gamma \in G$, $f \in \mathrm{Ind}_H^G W$, let $\gamma(f) : G \to W$, $g \mapsto f(g\gamma)$

  then $\gamma(f) \in \mathrm{Ind}_H^G W$: $hg \mapsto f(hg\gamma) = h f(g\gamma)$

Check: $\mathrm{Ind}_H^G W$ becomes a G-rep this way.

Remark: $\dim_{\mathbb{C}}(\mathrm{Ind}_H^G W) = (G:H) \cdot \dim_{\mathbb{C}} W$



Thm: (Frobenius reciprocity)

V G-rep, W H-rep

$$\mathrm{Hom}_G(V, \mathrm{Ind}_H^G W) \cong \mathrm{Hom}_H(V|_H, W)$$