MATH 570: Higher Algebra I

Prof. Eyal Z. Goren

Lecture notes by A. Tomberg

Fall 2010
McGill University

Table of contents

September-15-10
12:19 PM

§ 1.a. Language of categories

September-06-10
1:46 PM

<u>Def</u>: A category C consists of objects, morphisms and a composition law.

* A collection objects of C is denoted $Obj(C)$. They need not form a set.

* $\forall A, B \in Obj(C)$, a set $Hom(A,B)$ of morphisms from A to B. Notation:

$$f \in Hom(A,B) \iff f : A \to B \iff A \xrightarrow{f} B$$

However f need not be a function!

* The composition map

$$\begin{aligned} Hom(A,B) \times Hom(B,C) &\longrightarrow Hom(A,C) \\ (f,g) &\longmapsto g \circ f \end{aligned}$$

with the following properties:

1. $(A,B) \neq (A',B') \implies Hom(A,B) \cap Hom(A',B') = \phi$

2. $\forall A \in Obj(C)$, $\exists\, 1\!\!1_A \in Hom(A,A)$ s.t.

   $\forall f : Hom(A,B)$, $f \circ 1\!\!1_A = f$, $1\!\!1_B \circ f = f$

3. Associativity of composition
   $$f \circ (g \circ h) = (f \circ g) \circ h$$

Examples

1. Sets : objects $\longrightarrow$ sets
   morphisms $\longrightarrow$ functions
   composition $\longrightarrow$ function composition

2. Groups : objects $\longrightarrow$ groups
   morphisms $\longrightarrow$ group homo'
   composition $\longrightarrow$ usual one.

3. K-vector sp. (K is a fixed field)

   objects $\longrightarrow$ v.sp. over K
   morphisms $\longrightarrow$ linear maps
   composition $\longrightarrow$ usual composition

Def: Let C be a category, $f: A \to B$ a morphism. We say that f is an isomorphism (abbreviated 'iso') if $\exists g: B \to A$ s.t.

$$g \circ f = 1\!\!1_A \quad \text{and} \quad f \circ g = 1\!\!1_B$$

Def: An initial object in a category C is an object A s.t. $\forall B \in Obj(C)$, $\exists!$ morphism $f: A \to B$.

Claim: If an initial object exists, it is unique up to a unique iso, i.e. if A_1, A_2 are initial objects, $\exists!$ iso $f: A_1 \to A_2$.

Proof: Let A_1, A_2 be initial objects. By definition, $\exists!\ f: A_1 \to A_2$ and $\exists!\ g: A_2 \to A_1$.

Hence, $g \circ f \in \mathrm{Hom}(A_1, A_1)$, but $1\!\!1_{A_1} \in \mathrm{Hom}(A_1, A_1)$ too. Thus, as A_1 is an initial object,

$$g \circ f = 1\!\!1_{A_1}$$

Similarly, $f \circ g = 1\!\!1_{A_2} \Longrightarrow g$ & f are iso. $\square$

Def: A *final object* in a category C is an object A s.t. $\forall B \in \mathrm{Obj}(C)$, $\exists!\ f: B \to A$

Claim: If a final object exists, it is unique up to a unique iso.

Proof: Exercise.

Examples

1. In **Sets**, $\emptyset$ is an initial object and any $\{*\}$ (singleton) is a final object.

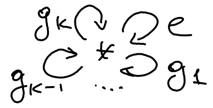
2. In $\underline{\text{Groups}}$, the trivial group $\{e\}$ is both an initial and a final object, such objects are called the zero objects.

3. In $\underline{K-\text{v.sp.}}$, the zero object is $\{0\}$

4. Let G be a group and define a category C as follows.

- $\text{Obj}(C) = \{*\}$ (any object)

- $\text{Hom}(*,*) = G$



- Composition $g \circ f = gf$ (group product)

$\mathbb{1}_* = e_G$ (this category has a group structure)

$\therefore$ Unless $G = \{e\}$, there is no initial, nor final object in C.

§ 1.b. Universal objects

September-06-10
8:08 PM

Def: Let C be a category and $A, B \in Obj(C)$

A product for A & B is an object D with morphisms

$$\begin{tikzcd} & D \arrow[dl, "f_A"'] \arrow[dr, "f_B"] & \\ A & & B \end{tikzcd}$$

which is universal for this property, that is

$\forall E \in Obj(C)$ with
$$\begin{tikzcd} & E \arrow[dl, "g_A"'] \arrow[dr, "g_B"] & \\ A & & B \end{tikzcd}$$

$\exists !$ morphism $h : E \to D$ such that the following diagram commutes.

$$\begin{tikzcd} & E \arrow[ddl, "g_A"'] \arrow[d, "h"] \arrow[ddr, "g_B"] & \\ & D \arrow[dl, "f_A"] \arrow[dr, "f_B"'] & \\ A & & B \end{tikzcd}$$

i.e. $f_A \circ h = g_A$ and $f_B \circ h = g_B$.

Claim: If a product for A, B exists, it is unique, up to a unique iso.

Proof: Let
$$\begin{tikzcd} & D_1 \arrow[dl, "f_A^1"'] \arrow[dr, "f_B^1"] & \\ A & & B \end{tikzcd}
\quad \text{and} \quad
\begin{tikzcd} & D_2 \arrow[dl, "f_A^2"'] \arrow[dr, "f_B^2"] & \\ A & & B \end{tikzcd}$$
be products.

By using the universal property twice, we find morphisms h_1 and h_2:

$$\begin{tikzcd} D_1 \arrow[rr, bend right, "h_1"'] \arrow[d, "f_A^1"'] \arrow[drr, "f_B^1" near end] & & D_2 \arrow[ll, bend right, "h_2"'] \arrow[d, "f_B^2"] \arrow[dll, "f_A^2"' near end] \\ A & & B \end{tikzcd}$$

We will show that h_1, h_2 are iso's. Consider

$$\begin{tikzcd} & D_1 \arrow[dl, "f_A^1"'] \arrow[d, "h_2 \circ h_1"] \arrow[dr, "f_B^1"] & \\ A & D_1 \arrow[l, "f_A^1"] \arrow[r, "f_B^1"'] & B \end{tikzcd}$$

This diagram commutes, b/c

$$f_A^1 \circ (h_2 \circ h_1) = (f_A^1 \circ h_2) \circ h_1 \overset{\text{By univ. prop. for } D_2}{=} f_A^2 \circ h_1 \underset{\text{By univ. prop. for } D_1}{=} f_1^A$$

Similarly, $f_B^1 \circ (h_2 \circ h_1) = f_B^1$.

But $\mathbb{1}_{D_1} : D_1 \to D_1$ also makes this diagram commute. So, by uniqueness requirement, $h_2 \circ h_1 = \mathbb{1}_{D_1}$

Similarly, $h_1 \circ h_2 = \mathbb{1}_{D_2}$. $\square$

From now on will denote the product by $A \sqcap B$.

Examples

1. Sets : $A \sqcap B = A \times B$, the cartesian product with projection maps.

2. Groups : $A \sqcap B = A \times B$, direct product of groups with projection maps.

3. K-v.sp. : $A \sqcap B = A \times B$, direct product of v. sp. with projections.

Def: In a category C, a coproduct of A, B is an object D with morphisms

$$\begin{tikzcd} A \arrow[r, "f_A"] & D & B \arrow[l, "f_B"'] \end{tikzcd}$$

universal for this property, i.e. $\forall E \in Obj(C)$ with morphisms

$$\begin{tikzcd} A \arrow[r, "g_A"] & E & B \arrow[l, "g_B"'] \end{tikzcd}$$

$\exists! \, h : D \to E$ making the following diagram commute :

$$\begin{tikzcd} A \arrow[r, "f_A"] \arrow[dr, "g_A"'] & D \arrow[d, "h"] & B \arrow[l, "f_B"'] \arrow[dl, "g_B"] \\ & E & \end{tikzcd}$$

Claim: If a coproduct of A, B exists, it is unique up to a unique iso.

Proof: Exercise.

We denote the coproduct by $A \sqcup B$

Examples

1. **Sets**: $A \sqcup B$ = disjoint union of A & B.

$A \sqcup B = A \times \{1\} \cup B \times \{2\}$ is a good definition that works even if $A = B$.

canonical injections.

$$\begin{tikzcd} A \arrow[r, "i_A"] \arrow[dr, "g_A"'] & A \sqcup B \arrow[d, "h"] & B \arrow[l, "i_B"'] \arrow[dl, "g_B"] \\ & E & \end{tikzcd}$$

where $h(x) = \begin{cases} g_A(x) & \text{if } x \in A \\ g_B(x) & \text{if } x \in B \end{cases}$

2. **K-v.sp.** $A \sqcup B = A \times B \ (= A \sqcap B)$ cartesian product of v.sp.

$$A \xrightarrow{i_A} A \times B \xleftarrow{i_B} B \qquad \begin{aligned} i_A(a) &= (a, 0) \\ i_B(b) &= (0, b) \end{aligned}$$

$$\begin{tikzcd}
A \arrow[r, "i_A"] \arrow[dr, "g_A"'] & A \times B \arrow[d, "h"] & B \arrow[l, "i_B"'] \arrow[dl, "g_B"] \\
& E &
\end{tikzcd}$$

Forced on us is
$$\begin{cases} h(a,0) = g_A(a) \\ h(0,b) = g_B(b) \\ h \text{ a linear map.} \end{cases}$$

$\therefore$ The only possibility is

$$h(a,b) = h(a,0) + h(0,b) = g_A(a) + g_B(b).$$

3. <u>Groups</u>: Let A, B be groups.

First, note that $A \sqcup B \neq A \times B$, as if

$$A = B = \mathbb{Z}_2, \quad A \times B = \mathbb{Z}_2 \times \mathbb{Z}_2$$

Take $E = S_3$ with group homo`

$$\begin{tikzcd}
A \arrow[r] \arrow[dr, "1 \mapsto (12)"'] & A \times B \arrow[d, "h?"] & B \arrow[l] \arrow[dl, "1 \mapsto (13)"] \\
& E &
\end{tikzcd}$$

If h exists, $h(1,0) + h(0,1) = h(11) = h(0,1) + h(1,0)$, but $(12)(13) \neq (13)(12)$ in S_3. $\times\!\!\!\times$

There is a coproduct in groups, but we will discuss it later.

§ 2.a. Groups

September-07-10
9:55 AM

Recall: Let G be a group, with associative group product:

$$G \times G \longrightarrow G$$
$$(g, h) \longmapsto gh$$

* $\exists\, e_G = 1_G = e = 1$ (or 0_G if G is abelian), such that

$$\forall g \in G, \quad eg = ge = g$$

* $\forall g \in G,\ \exists g^{-1} \in G$ s.t. $gg^{-1} = g^{-1}g = e$,

* $H \subseteq G$ is called a subgroup $(H < G)$ if $e_G \in H$ and $(x, y \in H \Rightarrow xy \in H$ and $x^{-1} \in H)$

* $f: G_1 \to G_2$ is a group homomorphism (homo) if $f(xy) = f(x)f(y)$ $\forall x, y \in G_1$.

↳ Properties of group homo:

- $f(e_{G_1}) = e_{G_2}$
- $f(x^{-1}) = (f(x))^{-1}$
- $\mathrm{Ker}(f) = \{g \in G_1 : f(g) = e_{G_2}\}$ is a subgroup of G_1.

- f is injective $\iff \ker(f) = \{e_{G_1}\}$
- f is an iso $\iff f$ is bijective.

Proposition: Let $H < G$, then TFAE

① $\forall g \in G$, $gH = Hg$, where

$\begin{cases} gH \text{ is the left coset} : \{gh : h \in H\}, \\ Hg \text{ is the right coset} : \{hg : h \in H\}. \end{cases}$

② $\forall g \in G$, $gHg^{-1} = H$.

③ $\forall g \in G$ $gHg^{-1} \subseteq H$.

④ $\exists$ group A & a group homo $f : G \longrightarrow A$ s.t.

$$\ker(f) = H.$$

Such subgroups are called normal, and we write $H \triangleleft G$.

Given $H \triangleleft G$, we construct the quotient group G/H as follows.

$$G/H = \{gH : g \in G\} \text{ with the product}$$

$$(g_1H)(g_2H) := (g_1g_2)H \text{, well defined.}$$

Note that $x \neq y \not\Rightarrow xH \neq yH$ in general.

The identity element is $H = eH$ and the inverse is

$$(gH)^{-1} := g^{-1}H$$

Often we write $\overline{g}$ for the coset gH, then the group law becomes:

$$\overline{g_1}\,\overline{g_2} = \overline{g_1 g_2}, \quad \overline{e_G} = e_{G/H}, \quad (\overline{g})^{-1} = \overline{g^{-1}}$$

The map
$$\begin{aligned} \pi : G &\longrightarrow G/H \\ g &\longrightarrow \overline{g} \end{aligned}$$
is a group homo' with kernel H.

Isomorphism Theorems

Theorem: First iso' theorem.

Let $f : G_1 \to G_2$ be a group homo' with kernel H. Let $N \lhd G_1$, $N \subseteq H$.

Then $\exists!$ group homo' $F : G_1/N \longrightarrow G_2$ s.t. the diagram below commutes.

$$\begin{tikzcd} G_1 \arrow[rr, "f"] \arrow[dr] & & G_2 \\ & G_1/N \arrow[ur, "F"'] & \end{tikzcd}$$

Furthermore, the $\ker(F) = H/N \subseteq G/N$,

i.e. $\{hN : h \in H\} \subseteq \{gN : g \in G\}$.

Proof (sketch):

1. Define $F(gN) = f(g)$, well-defined?

$gN = \tilde{g}N \iff g^{-1}\tilde{g} \in N$, then

$$f(\tilde{g}) = f(gg^{-1}\tilde{g}) = f(g)\,\cancel{f(g^{-1}\tilde{g})}^{\,e} = f(g) \checkmark$$

2. F a group homo?

3. $\ker(F) = \{gN : f(g) = e_{G_2}\} =$

$= \{gN : g \in H\} = H/N$

$\square$

Corollary: If f is surjective,

$$G_1/H \cong G_2,$$

because F is also surjective and

$\ker(F) = H/H \cong \{e_{G_1/H}\} \implies F$ iso $\checkmark$

If $f : G_1 \longrightarrow G_2$ is a group homo'

$$H < G_1 \implies f(H) < G_2$$

$$H < G_2 \implies f^{-1}(H) < G_1$$

<u>Theorem</u> : Second iso' theorem.

Let $A < G$, $B \triangleleft G$, then

$$AB = \{ab : a \in A, b \in B\} < G \text{ and}$$

$$AB/B \cong A/A \cap B$$

(in particular $A \cap B \triangleleft A$).

<u>Proof</u> (sketch):

1. $AB/B = \pi(A)$, $\pi : G \longrightarrow G/B$, and
   $AB = \pi^{-1}(AB/B)$, so it is a group.
2. $A \longrightarrow AB/B$, $a \longmapsto aB$ comes from $\pi|_A$, so it is a group homo'.
   surjective b/c $AB/B = \{aB : a \in A\}$
   kernel $= \{a \in A : aB = B$, i.e. $a \in A\} = A \cap B$.
3. Apply the 1st iso' thm. $\square$

Theorem: Third iso theorem

Let $A, B \lhd G$, $A \subseteq B$, then

$$(G/A)/(B/A) \cong G/B$$

Proof: (sketch)

? 1. Let $\pi : G \longrightarrow G/B$ be the canonical injection map with $\ker(\pi) = B \supseteq A$

2. The map $f : G/A \longrightarrow G/B$, $gA \xmapsto{f} gB$ has kernel $B/A = \{gA : g \in B\}$.

3. Apply 1^{st} iso theorem to

$$\begin{tikzcd}
G/A \arrow[rr, "f"] \arrow[dr] & & G/B \\
& (G/A)/(B/A) \arrow[ur, "F"'] &
\end{tikzcd}$$

$\Longrightarrow \ker(F) = (B/A)/(B/A) \cong \{e\}$

$\Longrightarrow F$ is an iso.

$\square$

Theorem: Fourth iso theorem.

Let $f: G_1 \to G_2$ be a surjective homo with kernel K. Then $\exists$ bijection

$$F: \{A \mid A < G_1,\ A \supseteq K\} \longrightarrow \{B : B < G_2\}$$

given by $H \xmapsto{F} f(H)$

Furthermore, F takes normal subgroups to normal subgroups.

Proof:

?

b

§ 2.b. Group actions on sets

September-10-10
11:15 AM

G – group, S – set

Def: The action of G on S is a map

$$G \times S \longrightarrow S$$
$$(g, s) \longrightarrow g * s \quad (\text{or } gs)$$

such that $\forall s \in S$ and $\forall g, g' \in G$,

$$1 * s = s$$
$$(gg') * s = g * (g' * s)$$

For every set S, we can define its permutation group

$$\Sigma_S = \{ f : S \to S \mid f \text{ is bijective} \}$$

Perversely, we write S_n for the group of permutations of $\{1, \dots, n\}$.

Σ_S is a group with the product given by the composition, and identity function acting as identity element.

Notice that to give an action of a group G on a set S is equivalent to giving a group homo' $\varphi : G \longrightarrow \Sigma_S$.

Proof: (sketch)

Given an action, set $\Psi: G \to \Sigma_S$ be defined by
$$(\Psi(g))(s) = g * s$$
$\Psi(g)$ is clearly surjective and since
$$g * s_1 = g * s_2 \implies s_1 = g^{-1} g\, s_2 = s_2$$
it is also injective.

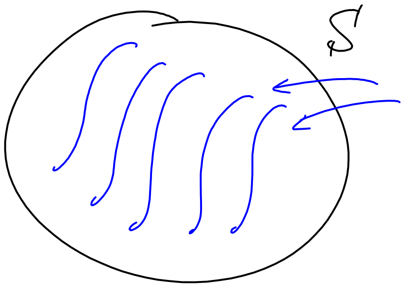
Conversely, given $\Psi: G \to \Sigma_S$, define
$$g * s = \Psi(g)(s)$$
$\square$

Def: For $s \in S$, define
$$Orb(s) = \{ g*s : g \in G \} \subseteq S$$
$$Stab(s) = \{ g \in G : g*s = s \} < G$$

Claim: Two orbits are either equal or disjoint.

Proof: Suppose $Orb(s_1) \cap Orb(s_2) \neq \emptyset \implies$
$$\implies g_1 * s_1 = g_2 * s_2 \implies s_1 = g_1^{-1} g_2 * s_2 \in Orb(s_2)$$
$$\implies \forall g \in G,\ g * s_1 = (g g_1^{-1} g_2) * s_2 \in Orb(s_2)$$
$$\implies Orb(s_2) \supseteq Orb(s_1).$$

By symmetry $\mathrm{Orb}(s_2) = \mathrm{Orb}(s_1)$. $\square$



<u>Lemma</u> : $\exists$ bijection

$$F : \underbrace{G/\mathrm{Stab}(s)} \longrightarrow \mathrm{Orb}(s)$$

not a quotient group, but a collection of cosets!

<u>Proof</u>: Let $H = \mathrm{Stab}(s)$, define F by

$$xH \xmapsto{F} x * s$$

- well-defined : if $xH = yH$, $y = xh$ for some $h \in H$,

$$y * s = (xh) * s = x * (h * s) = x * s \checkmark$$

- clearly surjective $\checkmark$
- injective : $x_1 * s = x_2 * s \Rightarrow s = x_1^{-1} x_2 * s$
  $\Rightarrow x_1^{-1} x_2 \in H \Rightarrow x_1 H = x_2 H \checkmark$

$\square$

Corollary: if G is finite

$$\#\,\mathrm{Orb}(s) = \frac{\#G}{\#\mathrm{Stab}(s)}$$

Theorem: Lagrange's theorem

Let G be a finite group, $H < G$, then

$$\#H \mid \#G \quad \text{and} \quad \frac{\#G}{\#H} = \#\{\text{left cosets of } H\} = \#\{\text{right cosets of } H\}.$$

Proof: Let H act on G by

$$\begin{aligned} H \times G &\longrightarrow G \\ (h,g) &\longrightarrow hg \end{aligned}$$

Choose representatives $\{x_i\}$ for the orbits.

$$G = \bigsqcup_{i=1}^{N} \mathrm{Orb}(x_i) = \bigsqcup_{i=1}^{N} Hx_i$$

For each i, $$|\mathrm{Orb}(x_i)| = \frac{\#H}{\underbrace{\#\mathrm{Stab}\{x_i\}}_{=\{e\}}} = \#H$$

$\therefore$ Every coset has the same cardinality

$$\Longrightarrow \#G = \underbrace{N}_{\#\text{ of cosets}} \cdot \#H$$

As $(xH)^{-1} = Hx^{-1}$, the last statement follows.

Class equation

September-08-10
10:09 AM

G – finite group.

G acts on itself by conjugation.

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, h) &\longmapsto ghg^{-1} \end{aligned}$$

▷ $e * h = ehe^{-1} = ehe = h$

▷ $(g_1 g_2) * h = g_1 g_2 h (g_1 g_2)^{-1} = g_1 g_2 h g_2^{-1} g_1 =$
$= g_1 * (g_2 * h)$

The orbit of $h \in G$ under this action is called its conjugacy class, i.e. the set

$$\{ghg^{-1} : g \in G\}$$

Note: $\mathrm{Orb}(h) = \{h\}$ iff $\forall g,\ ghg^{-1} = h$

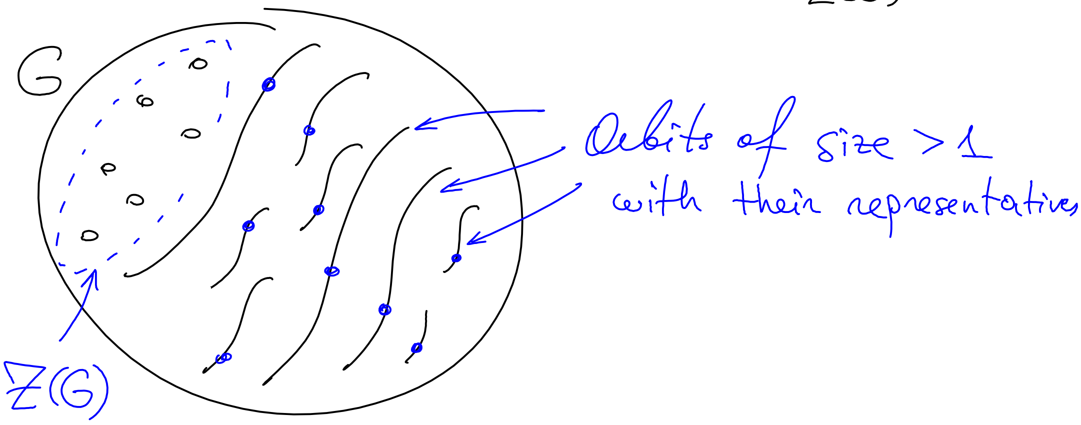
$\iff gh = hg \quad \forall G \iff h \in Z(G)$

the center of G

Exercise: Check that $Z(G) \lhd G$

The partition of G relative to this action is

$$G = \left[\bigsqcup_{h \in Z(G)} \{h\} \right] \sqcup \left[\bigsqcup_{\substack{x \text{ representative,} \\ x \notin Z(G)}} Orb(x) \right]$$



Def: For $x \in G$, define the centralizer of x in G by

$$C_x(G) = \{ g : gxg^{-1} = x \} = \underset{\uparrow}{Stab}(x)$$

relative to the conjugation action

$\therefore$ The class equation becomes

$$\#G = \#Z(G) + \sum \frac{\#G}{C_x(G)}$$

where the sum is taken over all x that are representatives of conjugacy classes of size larger than one.

§ 2.c. p-Groups

September-10-10
9:09 PM

Def: Let p be a prime. A group G is called a *p-group* if

$$\#G = p^r, \quad r \geq 1$$

Theorem: Every p-group has a non-trivial center.

↳ Consequence: G, Z_G and G/Z_G are p-grps
$\Rightarrow$ useful for induction.

Proof: By the class equation

$$1 < \underset{\substack{\uparrow \\ \text{divisible by } p}}{p^r} = \#Z_G + \underbrace{\sum_{\substack{\text{rep. } \{x\} \\ x \notin Z_G}} \frac{p^n}{C_G(x)}}_{\text{divisible by } p}$$

$\therefore \; p \mid \#Z_G \Rightarrow \#Z_G \geq p > 1$

$\Rightarrow Z_G \neq \{e\}$ $\square$

Theorem: G – a p-group, $\#G = p^n$.

(1) Let $H \lneq G$, then $\exists K \trianglelefteq G$, $H \subseteq K$ and $[K : H] = p$.

② $\exists H_i \triangleleft G$ s.t. $\# H_i = p^i$ and

$$\{e\} \subseteq H_1 \subseteq H_2 \subseteq \dots \subseteq H_{r-1} \subseteq G$$

<u>Recall</u>: $[G:H] = \#$ of cosets of H in G.

<u>Proof of Theorem</u>

① Consider $G \xrightarrow{\pi} G/H$ a p-group!

Let $x \in Z_{G/H}$, $x \neq e_{G/H}$, then

$$y = x^{\mathrm{ord}(x)/p} \text{ has order } p.$$

Recall that $\mathrm{Order}(x) = \min\{k > 0 : p^k = e\}$.

So, the cyclic subgroup $\tilde{K}$ generated by y
$\tilde{K} = \langle y \rangle = \{e, y, y^2, \dots, y^{p-1}\}$
has exactly p elements.

Moreover, $x \in Z_{G/H} \Rightarrow \tilde{K} \subseteq Z_{G/H}$
$\Rightarrow \tilde{K} \triangleleft G/H$

Thus, by 4th iso theorem $K := \pi^{-1}(\tilde{K}) \triangleleft G$

Obviously, $K \supseteq H$ and $\# K = \# \tilde{K} \cdot \# H$
$\Rightarrow [K:H] = p$. ✓

② Follows by repeatedly applying ①, starting with $H = \{e\}$.

$\square$

Examples

1. $\# G = p$. As p is prime, $\forall x \in G$, $x \neq e$

$$\langle x \rangle = G \implies G \cong \mathbb{Z}_p$$

Exercise: Let G be a group, $H < G$, $H \subseteq Z_G$ such that G/H is cyclic. Prove that G is abelian.

2. $\# G = p^2$. Then, G is abelian.

Indeed $Z_G \neq \{e\} \implies \exists H \subseteq Z_G$, $H < G$, $\# H = p$ $\implies \# G/H = p \implies G/H$ is cyclic. By the exercise above, G must be abelian.

Hence, there are two possibilities

a) $G \cong \mathbb{Z}_{p^2}$, if $\exists g \in G$, $\mathrm{ord}(g) = p^2$)

b) $G \cong (\mathbb{Z}_p)^2$, since every non-trivial elt has order p.

$\hookrightarrow$ In this case, we can view G as a vector sp. over the field $\mathbb{Z}_p$. (simply check the axioms)

Then G must have $\dim = 2$ (b/c $\# G = p^2$), so it is iso to $(\mathbb{Z}_p)^2$.

3. $\#G = p^3$. Similarly to the above case, if G is abelian, there are three possibility:

a) $G \cong \mathbb{Z}_{p^3}$, if $\exists\, x \in G$, $\mathrm{ord}(x) = p^3$

b) $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_p$, if $\max\limits_{x \in G} \{\mathrm{ord}(x)\} = p^2$

c) $G \cong (\mathbb{Z}_p)^3$, otherwise.

If G is not abelian, by the contrapositive of the exercise, $\# Z_G = p$. Moreover,

$$G/Z_G \cong (\mathbb{Z}_p)^2,$$

because it cannot be cyclic! In fact, there are precisely two such groups (up to iso', of course). One of them is

$\left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{Z}_p \right\}$ with the mult. given by

$$\begin{pmatrix} 1 & x_1 & y_1 \\ & 1 & z_1 \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & x_2 & y_2 \\ & 1 & z_2 \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & x_1 + x_2 & y_1 + y_2 + x_1 z_2 \\ & 1 & z_1 + z_2 \\ & & 1 \end{pmatrix}$$

non abelian term

And $\exists$ surjective homo' $G \longrightarrow (\mathbb{Z}_p)^2$

$$\begin{pmatrix} 1 & x & y \\ & 1 & z \\ & & 1 \end{pmatrix} \longmapsto (x, z)$$

with kernel $= Z_G$.

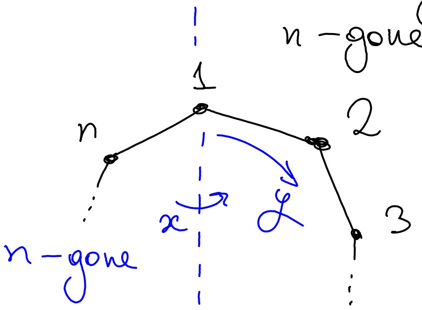
Exercise (Groups of small order)

$\# G$	Iso classes of groups
1	$\{e\}$
$n = 2,3,5,7$	$\mathbb{Z}_n$
4	$\mathbb{Z}_4$, $(\mathbb{Z}_2)^2$
6	$\mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2$

Show that $\exists$ precisely 5 groups of order $8 = 2^3$, up to iso.

(*Hint*: The two non-abelian ones are D_8 & Q_8.)

Recall: The dihedral group on $2n$ elements (D_{2n}) is the group of symmetries of a regular n-gone.



Let x be a reflexion about an axis passing throug vertex 1, and y — a clockwise rotation by 1 step. Then,

$$x^2 = y^n = xyxy = 1,$$

and all other relations are consequences of those.

$$D_{2n} = \{e, y, y^2, \dots, y^{n-1}, x, xy, \dots, xy^{n-1}\}$$

Some properties:

→ $\langle y \rangle \triangleleft D_{2n}$

→ All elements outside of $\langle y \rangle$ are reflexions.
(i.e. all xy^i are reflexions)

→ There are n reflexions:

- If n is odd, every reflexion has a unique fixed vertex.

- If n is even, $n/2$ reflexions have 2 fixed vertices & $n/2$ others have none.

Recall: The quaternion group (Q or Q_8)

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

with relations $i^2 = j^2 = k^2 = -1$,
$ij = k$, $jk = i$, $ki = j$, and $ij = -ji$

The elements $\{\pm 1\}$ form the center ZQ

→ Every subgroup of Q is normal, but Q is not abelian.

Coset representation

September-15-10
12:12 PM

Let G be a group, $H < G$ and let G/H denote the collection of cosets xH. The action

$$G \times G \longrightarrow G/H$$
$$(g, xH) \longmapsto (gx)H$$

$$\mathrm{Stab}(xH) = \{ g : (gx)H = xH \} =$$
$$= \{ g : x^{-1} g x \in H \} =$$
$$= \{ g : g \in x H x^{-1} \} = x H x^{-1}$$

So the resulting homo'

$$G \longrightarrow \Sigma_{G/H}$$

has the kernel $K := \bigcap_{x \in G} x H x^{-1} \lhd G$

$K \subseteq H$ is, in fact, the largest normal subgroup contained in H.

Corollary: If $[G:H] = n$, then $\exists K \lhd G$, $K \subseteq G$ such that

$$[G:K] \mid n!$$

Proof: $G/K \hookrightarrow \Sigma_{G/H} \cong S_n$

canonical injection

$\# S_n = n!$

$\# G/K = [G:K] \mid n!$ by Lagrange.

$\square$

<u>Corollary</u>: G finite group and p, the minimum prime dividing $\# G$

Let $H < G$ be s.t. $[G:H] = p$, then

$$H \trianglelefteq G$$

<u>Proof</u>: Let $K \trianglelefteq G$ be as in the above corollary. $\# G/K \mid p!$

$$\# G/K = [G:K] = [G:H][H:K] = p\,[H:K]$$

$\Longrightarrow [H:K] \mid (p-1)!$ & $[H:K] \mid \# G$

$\Longrightarrow [H:K]$ is a product of primes $< p$ & it divides $\# G$. Contradiction! $\times$

$\therefore [H:K] = 1 \Longrightarrow H = K$

$\square$

<u>Exercises</u>: (1) Prove Cauchy – Frobenius formula (a.k.a. Burnside's lemma):

Let G be a finite group acting on a finite set S. Let $N = \#$ orbits.

Then $N = \frac{1}{\# G} \sum_{g \in G} \mathrm{Fix}(g)$

Where $\mathrm{Fix}(g) = \# \{ s \in S : g * s = s \}$
↳ # of fixed points.

Hint: Use the function
$$I(g,s) = \begin{cases} 1, & \text{if } g*s=s \\ 0, & \text{otherwise} \end{cases}$$
& change the order of summation.

(2) Give a formula for the number of different roulette wheels / necklace designs with n beads: k blue, (n-k) red.

→ necklace — symmetric under reflexions & rotations

→ roulette wheel — symmetric under rotations only.

Hint: Apply Cauchy-Frobenius formula.

§ 2.d. Sylow Theorem

September-15-10
12:11 PM

G – finite group, p – prime
$\#G = mp^r$, $r \geq 1$, $(m,p) = 1$

<u>Def</u>: A p-subgroup H of G is called maximal if $\forall$ p-subgroup J of G

$$H \subseteq J \implies H = J$$

<u>Lemma</u>: Let A be a finite abelian group s.t. $p \mid \#A$. The A has an element of order p.

<u>Proof</u>: By induction on $\#A$

- Base case $\#A = p$: Then $A \cong \mathbb{Z}_p \implies$ all elements have order p.

- General case: let $x \in A$, $x \neq \{e\}$.

If $p \mid \mathrm{ord}(x)$, $y = x^{\frac{\mathrm{ord}(x)}{p}}$ has order p.

Otherwise, $(p, \mathrm{ord}(x)) = 1$. Consider

$B = A/\langle x\rangle$, then $p \mid \#B$, so by induction hypothesis, $\exists z \in B$, $\mathrm{ord}(z) = p$

Lift z to y in A, i.e. $A \xrightarrow{\pi} A/\langle x\rangle$, $y = \pi^{-1}(z)$

$\implies p = \mathrm{ord}(z) \mid \mathrm{ord}(y) \implies y^{\frac{\mathrm{ord}(y)}{p}}$ has order p. $\square$

Proposition: G has a maximal p-subgroup of order p^r.

Proof: By induction on $\#G$.

- $\#G = p$ (base case), then G itself is a maximal p-subgroup of itself.

- General case.

→ **Case 1**: $p \mid \#Z_G$, then by lemma, $\exists x \in Z_G$, $\mathrm{ord}(x) = p$, $\langle x \rangle \triangleleft G$. Consider

$$H = G/\langle x \rangle, \quad \#H = p^{r-1} \cdot m$$

By induction hypothesis, H has a maximal p-subgroup K of order p^{r-1}, (if $p^{r-1} = 1$, let $K = \{e\}$).

Then the preimage of K under $G \to H$ is a subgroup of G of order p^r. ✓

→ **Case 2**: $p \nmid \#Z_G$

By the class equation,

$$\underbrace{\#G}_{\substack{\text{Divisible} \\ \text{by } p}} = \underbrace{\#Z_G}_{\substack{\text{Not divisible} \\ \text{by } p}} + \sum_{\substack{\{x\} \text{ rep'n} \\ \text{of conj. classes} \\ \text{of size} > 1}} \frac{\#G}{\#C_G(x)}$$

Since $p \nmid \#Z_G$, there must be another term not divisible by p on the RHS $\Rightarrow$

$$\Rightarrow \exists x : p \nmid \frac{\#G}{\#C_G(x)} \Rightarrow$$

$$\Rightarrow \#C_G(x) = p^r \cdot m' \ \& \ \underbrace{\#C_G(x) < \#G}.$$

↳ b/c conj. class has size > 1

∴ By induction hypothesis, $C_G(x)$ has a subgroup of order p^r & this subgroup is also a subgroup of G.

□

<u>Def</u>: Let $P < G$, define the normalizer of P by

$$N_G(P) = \{ x \in G : xPx^{-1} = P \} < G$$

Note that $P \subseteq N_G(P)$ and that $N_G(P)$ is the maximal subgroup of G, in which P is normal.

<u>Lemma</u>: Let Q be a p-subgroup of G and P — a maximal p-subgroup of G.

Then $Q \cap P = Q \cap N_G(P)$.

<u>Proof</u>: Let $H := Q \cap N_G(P)$. Then, as $H < N_G(P)$ & $P \triangleleft N_G(P)$, HP is a subgroup of $N_G(P) \Rightarrow HP < G$.

Obviously, $HP \supseteq P$ & $\#HP = \dfrac{\#H \cdot \#P}{\#H \cap P}$

As $H < Q$, H is a p-group, so is $P \implies$

$\implies HP$ is a p-group.

But P is the maximal p-subgroup of G, so that we must have $HP = P$.

$\implies \#H = \#H \cap P \implies$ As $P \leq N_G(P)$

$$Q \cap N_G(P) = H = H \cap P = Q \cap P$$

$\square$

<u>Theorem</u>: (Sylow theorem)

Every maximal p-subgroup of G has p^r elements and all such subgroups are conjugate in G. If a denotes the number of these subgroups, then

$$a \mid \#G \text{ and } a = 1 \bmod p$$

<u>Proof</u>: Let $P = P_1$ be a maximal p-subgroup with p^r elements, whose existence is guaranteed by the Proposition above.

Let $S = \{P_1, \dots, P_a\}$ be the set of all conjugates of P in G, i.e. $P_i = x_i P x_i^{-1}$ for some $x_i \in G$.

Obviously, each has order p^r.

<u>Note</u> : G acts transitively on S by conjugation, i.e. there is only one orbit.

$$\Longrightarrow \quad a \mid \# G.$$

Let Q be any maximal p-subgroup of G and consider the action of Q on S by conjugation.

$$\mathrm{Stab}(P_i) = Q \cap N_G(P_i) = Q \cap P_i \text{ by Lemma}$$

Note that by maximality of Q, $Q \cap P_i \subseteq P_i$ with equality iff $Q = P_i$.

$$\therefore \; \# \mathrm{Orb}_Q(P_i) = \frac{\# Q}{\# \mathrm{Stab}(P_i)} = \frac{\# Q}{\# Q \cap P_i}$$

First, set $Q = P = P_1$. Then

$$\mathrm{Stab}_Q(P_1) = P_1 \Longrightarrow \mathrm{Orb}_Q(P_1) = \{P_1\}$$

$$\forall i \neq 1, \quad Q \cap P_i = P \cap P_i \subsetneq P_i \quad b/c \quad P \neq P_i$$

$$\Longrightarrow \# \mathrm{Orb}_Q(P_1) = 1, \; \# \mathrm{Orb}_Q(P_i) = \frac{\# Q}{\# Q \cap P_i} = p^{\alpha}, \alpha > 0.$$

$$\Longrightarrow a \equiv 1 \bmod p \quad \text{as claimed} \quad (\star)$$

Second, let Q be any maximal p-subgroup, which is not in S.

$$\# \mathrm{Orb}_Q(P_i) = \# Q / \# Q \cap P_i$$

$Q \cap P_i \subseteq Q$ with equality iff $Q = P_i$.
So, by maximality, $Q \cap P_i \subsetneq Q$.

$\Longrightarrow$ The size of any orbit is divisible by p.

$\therefore$ $p \mid a$ $\Longrightarrow$ Contradiction to $(*)$ $\#$.

$\square$

Def: A p-Sylow subgroup of G is a maximal p-subgroup of G.

Equivalently, a p-Sylow subgroup is a subgroup of order p^r.

Rmk: A p-Sylow subgroup is normal in G iff there is exactly one p-Sylow subgroup in G.

Simple groups

September-15-10
12:17 PM

Def: G is called a simple group if its only normal subgroups are $\{e\}$ and G.

Example: • A group with p elements (p prime) is necessarily simple.

• Burnside's Theorem: A group order $p^\alpha q^\beta$

$p \neq q$, primes, and $\alpha + \beta > 1$,

is not simple [Hard!]

• Feit–Thompson Theorem: A finite group of odd order is not simple.
[Extremely Hard!]

• $A_n < S_n$ is simple for $n \geq 5$

$\# A_n = \frac{n!}{2}$, $\# A_5 = 60$.

Proposition: All groups G, $\# G < 60$ s.t. $\# G \neq 1$ and $\# G$ is not prime, are NOT simple.

That is $\exists H \triangleleft G$, $H \notin \{\{e\}, G\}$.

Proof: Let us list all numbers between 1 and 60, and cross out those for which the proposition is true.

~~1~~	~~2~~	~~3~~	~~4~~	~~5~~	~~6~~	~~7~~	~~8~~	~~9~~	~~10~~
~~11~~	12	~~13~~	~~14~~	~~15~~	~~16~~	~~17~~	18	~~19~~	20
21	22	~~23~~	24	~~25~~	26	~~27~~	28	~~29~~	30
~~31~~	~~32~~	33	34	35	~~36~~	~~37~~	38	39	40
~~41~~	42	~~43~~	44	45	46	~~47~~	48	~~49~~	50
51	52	~~53~~	54	55	56	57	58	~~59~~	

– primes & 1. (by

– groups of order p^r, because:

$\hookrightarrow$ by a previous result, a group of order p^r contain normal subgroups of all order p^a $(0 \leq a \leq r)$ $\Rightarrow$ NOT simple

– groups of order $p \cdot q^r$, $p<q$ primes, by the following result:

Lemma: $p<q$ primes, $r>0$, then the group of order $p \cdot q^r$.

Proof: Let Q be the q-Sylow subgroup. Then $Q \triangleleft G$ because $[G:Q]=p$, smallest prime dividing $\#G$.

Alternatively, # of q-Sylow subgroups, a, satisfies $a \mid p$ & $a = 1 \bmod q \Rightarrow a = 1$. $\square$

– groups of order p^2q, because

<u>Exercise</u>: Prove that the order p^2q is not simple.

<u>Hint</u>: Assume that both p & q - Sylow subgroups are not normal and count elements.

<u>Challenge</u>: Finish the proof

↳ One technique is to take a group of order say 24. Let P be a 2-sylow sgp.
$\Longrightarrow [G:P] = 3$

$$G \longrightarrow \Sigma_{G/P} \cong S_3 \quad \text{with kernel } K \triangleleft G$$

and $[G:K] = 6 \Longrightarrow K \neq \{e\}$
$K \subseteq P \Longrightarrow K \neq G$

$\therefore$ Groups of order 24 are not simple. $\square$

<u>Exercise</u>: Let G be of order pq, $p<q$ and $p \nmid (q-1)$.
Prove that G is a cyclic group.

<u>Hint</u>: Prove that it must be abelian, then use Chinese remainder thm.

§ 2.e. Solvable and nilpotent groups

September-15-10
12:17 PM

Assume G to be a finite group for this section.

Def: A normal series for G is

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_n = G$$

where $G_i \triangleleft G_{i+1}$ $\forall i$, but not necessarily $G_i \triangleleft G$!

Def: A group G is called solvable if there exists a normal series for G with

$$G_i / G_{i-1} \text{ abelian}, \quad \forall 0 \le i \le n-1$$

Motivation: 1. Finite group theory: "analyze G/H & H instead of H" philosophy.

2. Given a polynomial $x^m + a_{m-1}x^{m-1} + \dots + a_0$, we can associate to it a finite Galois group G. We can solve the polynomial in radicals iff G is solvable.

3. Solvable groups play a key role in the study of algebraic & Lie groups.

Example: $GL_n(\mathbb{R})$, a solvable subgroup is the Borel subgroup

$$\left\{ \begin{pmatrix} * & & * \\ & * & \\ 0 & & * \\ & & & * \end{pmatrix} \right\}$$

Proposition:

1. G solvable, $H < G$, then H is solvable.

2. G solvable; H – any group; $f : G \to H$, a group homo'. Then

$$f \text{ surjective} \implies H \text{ solvable.}$$

3. If $H \triangleleft G$ s.t. H & G/H are solvable, then G is solvable too.

Proof: Let $\{e\} = G_0 \triangleleft \dots \triangleleft G_n = G$ be a normal series for G with abelian quotients.

(1) $H < G \implies$ Let $H_i := G_i \cap H$, the obviously $H_0 = \{e\}$, $H_n = H$. Consider the homo'

$$H \cap G_i \hookrightarrow G_i \longrightarrow G_i / G_{i-1}$$

Its kernel is $H \cap G_i \cap G_{i-1} = H \cap G_{i-1}$, so that

$$H_{i-1} = H \cap G_{i-1} \triangleleft H \cap G_i = H_i$$

and $H \cap G_i / H \cap G_{i-1} \hookrightarrow G_i / G_{i-1}$

$\therefore$ H_i / H_{i-1} is iso to a subgroup of an abelian group $\Longrightarrow$ abelian. ✓

(2) $f : G \longrightarrow H$, a surjective homo.

Let $H_i = f(G_i)$, so that $H_0 = \{e_H\}$, $H_n = H$.

A surjective homo always maps normal subgroups to normal subgroups, so that

$$G_{i-1} \triangleleft G_i \xrightarrow[f|_{G_i} \text{ is surjective}]{} H_{i-1} \triangleleft H_i$$

We have $G_i \xrightarrow{f} H_i \xrightarrow{\pi} H_i / H_{i-1}$, surjective

$\operatorname{Ker}(f \circ \pi) \supseteq G_{i-1}$, so by 1^{st} iso thm,

$\exists$ well-defined surjective homo

$$G_i / G_{i-1} \longrightarrow H_i / H_{i-1}$$

$\therefore$ H_i / H_{i-1} is abelian (Exercise) ✓

(3) $\{e\} = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_a = H$
$\{e\} = K_0 \triangleleft K_1 \triangleleft \dots \triangleleft K_b = G/H$

Let $H_{a+i} = \pi^{-1}(K_i)$, where $G \xrightarrow{\pi} G/H$,
so that $H_{a+0} = H_a$, $H_{a+b} = G$, and

$$H_0 \lhd \cdots \lhd H_a < H_{a+1} < \cdots < H_{a+b} = G$$

As for $i \geq a$, H_i is the preimage of K_i under a surjective homo'

$$\begin{array}{ccc} H_{i+1} & \longrightarrow & K_{i+1} \\ \cup\!\vert & & \triangle \\ H_i & \longrightarrow & K_i \end{array}$$

$\therefore$ By 4th iso' thm, $H_i \lhd H_{i+1}$.

To see that H_{i+1}/H_i is abelian for $i \geq a$, consider the surjective homo'

$$H_{i+1} \twoheadrightarrow K_{i+1} \twoheadrightarrow \underbrace{K_{i+1}/K_i}_{\text{abelian}}$$

As $H_i \subseteq$ Kernel of that homo', by 1st iso' thm,

$$H_{i+1}/H_i \cong K_{i+1}/K_i$$

$\therefore$ H_{i+1}/H_i is abelian $\forall i$.

$\square$

Examples of solvable groups:

1. Any abelian group
2. Any p-group, b/c $\exists$ normal series with $[G_{i+1}:G_i] = p \Rightarrow G_{i+1}/G_i \cong \mathbb{Z}_p$ abelian.

3. Product of solvable groups is solvable

$$\left(A\times B \trianglerighteq A\times\{e\} \Longrightarrow \frac{A\times B}{A\times\{e\}} = B \right)$$

4. Any group of order less than 60 is solvable (proof by induction).

Def: Let G be a group. We define its commutator subgroup by

$$G' = \langle [x,y] \mid x,y\in G \rangle$$

where $[x,y] = xyx^{-1}y^{-1}$ is the commutator.

Fact: $\forall g\in G$, $g[x,y]g^{-1} = gxyx^{-1}y^{-1}g^{-1} =$

$$= gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} = [gxg^{-1}, gyg^{-1}]$$

Thus, $G' \trianglelefteq G$ and G/G' is abelian, b/c

$$\bar{x}\bar{y} = \bar{y}\bar{x} \iff \bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1} = e \iff [x,y] = e$$

In fact, if $H \trianglelefteq G$, G/H is abelian, then every commutator is trivial in $G/H \Longrightarrow$

$\Longrightarrow [x,y]\in H \Longrightarrow G' \subseteq H$.

Thus, we sometimes write

$$G/G' = G^{ab}$$ abelianization

Digression: Functors

September-28-10
5:16 PM

Let C, D be categories.

Def: A covariant (resp. contracovariant) functor $F : C \to D$ is a rule associating to each $A \in Obj(C)$, $F(A) \in Obj(D)$ and to each morphism $f : A_1 \to A_2$ in C, a morphism $F(f) : F(A_1) \to F(A_2)$ in D ($F(f) : F(A_2) \to F(A_1)$ for contracovariant functors) such that

$$F(1\!\!1_A) = 1\!\!1_{F(A)} \ \& \ F(f \circ g) = F(f) \circ F(g)$$
$$(\text{resp. } F(f \circ g) = F(g) \circ F(f)).$$

Examples

① Forgetfull functor $F : \underline{Groups} \to \underline{Sets}$

$F(A) =$ the underlying set of group A
$F(f) = f$ as a function on sets.

$\Longrightarrow F$ "forgets" about multiplication.

② $F : \underline{Groups} \longrightarrow \underline{Abelian\ Groups}$

$$F(G) = G^{ab} = G/G'$$

What about $F(f)$ for $f : G \to H$?

$$f([x,y]) = [f(x), f(y)] \Rightarrow f(G') \subseteq H'$$

Let $\psi : G \to G/G'$ be the canonical map
$\ker(\psi) \supseteq G' \Rightarrow$ By 1st iso thm,

$\exists F : G/G' \to H/H'$ s.t. $(F(f))\bar{g} = \overline{f(g)}$

<u>Exercise</u> : Verify that this defines a covariant functor.

(3) $F : \underline{K \text{ v-sp.}} \longrightarrow \underline{K \text{ v-sp.}}$

$F(V) = V^* = \mathrm{Hom}(V, K)$ (the dual v-sp.)

& $F(T) = T^*$, where if $T : V \to W$,

$T^* : W^* \to V^*$, $(T^*\varphi)(v) = \varphi(Tv)$

↳ Contracovariant functor.

(4) F : <u>Topological sp.</u> $\longrightarrow$ <u>Abelian groups</u>

$$F(X) = \begin{cases} H_i(X, \mathbb{Z}) & \leftarrow \text{covariant} \\ H^i(X, \mathbb{Z}) & \leftarrow \text{contracovariant} \end{cases}$$

Also F : <u>Pointed Topo. sp.</u> $\longrightarrow$ <u>Groups</u>

$F((X, x_0)) = \pi(X, x_0)$ ← the fundamental group

↳ Covariant functor.

Back to solvable groups

Let G be a finite group.

Def: The derived series of G is defined as

$$G^{(0)} = G, \quad G^{(1)} = G', \ldots, \quad G^{(i)} = [G^{(i-1)}]'$$

Then, by our previous results

$$G = G^{(0)} \triangleright G^{(1)} \triangleright \ldots \triangleright G^{(i)} \triangleright \ldots$$

is a normal series with abelian quotients, but it need not be the case that $\exists n$ s.t. $G^{(n)} = \{e\}$. If such n exists, G is solvable!

Proposition: If G is solvable, $\exists n : G^{(n)} = \{e\}$.

Proof: Let $G = H^0 \triangleright \ldots \triangleright H^n = \{e\}$ be a normal series with abelian quotients.
We show by induction that $H^i \supseteq G^{(i)}$

* $H^0 = G^{(0)}$
* Suppose $H^i \supseteq G^{(i)}$, then H^i/H^{i+1} abelian $\Longrightarrow$
$\Longrightarrow H^{i+1} \supseteq (H^i)' \supseteq (G^{(i)})' = G^{(i+1)}$ ✓

$\therefore \{e\} = H^n \supseteq G^{(n)} \Longrightarrow G^{(n)} = \{e\}$

$\square$

Exercise: Prove that G is solvable iff there exists a normal series with cyclic quotients.

Def: A group G is called supersolvable if it has a normal series

$$\{e\} = G_0 \triangleleft \dots \triangleleft G_n = G \ , \quad G_{i+1}/G_i \text{ cyclic},$$

and s.t. $G_i \triangleleft G \ \forall i \leq n$.

Exercise: Prove that S_4 is solvable, but not supersolvable.

↳ **Hint**: A subgroup $H < G$ is normal iff it is the union of G conjugacy classes.
In S_n, two permutations are conjugate if they have the same cycle type decomposition:

$\sigma = \sigma_1 \sigma_2 \cdots \sigma_k$ disjoint cycles of lengths $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k \geq 1$; $\sum \lambda_i = n$

Then $(\lambda_1, \dots, \lambda_k)$ is the cycle type decomposition of σ. It is a partition of n.

§ 2.f. Nilpotent groups

September-28-10
6:01 PM

Def: Let $H, K < G$, we define the commutator of H and K by

$$[H,K] = \langle [h,k] : h \in H, k \in K \rangle = [K,H]$$

Then $[H,K] < G$.

Let G be a finite group. Define

$$\gamma_0(G) = G \quad , \dots , \quad \gamma_{i+1}(G) = [\gamma_i(G), G]$$

Warning! Many books start at 1, not at 0!

So, $\gamma_0(G) = G \qquad = G^{(0)}$
$\gamma_1(G) = [G,G] = G' \qquad = G^{(1)}$
$\gamma_2(G) = [G',G] \qquad \neq G^{(2)} = [G',G']$!

$\longrightarrow$ The two series deviate from each other.

We will show that $\gamma_0(G) \triangleright \gamma_1(G) \triangleright \dots$, that γ_i/γ_{i-1} is abelian, and that $\gamma_i(G) \triangleleft G$

Def: If $\exists n$ s.t. $\gamma_n(G) = \{e\}$, we say that G is nilpotent. The minimum such n is called the nilpotence class of G.

For example $n=0 \Leftrightarrow G = \{e\}$ and $n = 1 \Leftrightarrow$
$\Leftrightarrow G \neq \{e\}$, G abelian.

Proposition: Some properties of $\gamma_i(G)$

1. $\gamma_{i+1}(G) \subseteq \gamma_i(G)$

2. $\gamma_i(G) \triangleleft G$

3. $\gamma_i(G) / \gamma_{i+1}(G)$ is abelian

Proof:

1. By induction $\gamma_1(G) \subseteq G = \gamma_0(G)$ ✓

If $\gamma_i(G) \subseteq \gamma_{i-1}(G)$, $\underbrace{[\gamma_i(G), G]}_{\gamma_{i+1}(G)} \subseteq \underbrace{[\gamma_{i-1}(G), G]}_{\gamma_i(G)}$ ✓

2. Also by induction: $\gamma_0(G) = G \triangleleft G$ ✓

Suppose $\gamma_{i-1}(G) \triangleleft G$, then $x \gamma_i(G) x^{-1} =$

$$= x < [a,b] : a \in \gamma_{i-1}(G), b \in G > x^{-1} =$$
$$= < [xax^{-1}, xbx^{-1}] : a \in \gamma_{i-1}(G), b \in G > \overset{\text{by ind. hyp.}}{=}$$
$$= < [y, g] : y \in \gamma_{i-1}, g \in G > = \gamma_i(G)$$ ✓

3. Enough to show that

$\gamma_{i+1}(G) \subseteq (\gamma_i(G))'$, but this is clear as

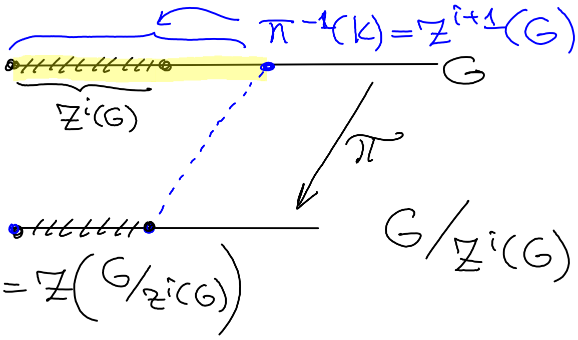
$$(\gamma_i(G))' = [\gamma_i(G), \gamma_i(G)] \underset{\text{b/c } \gamma_i(G) \subseteq G}{\subseteq} [\gamma_i(G), G] = \gamma_{i+1}(G)$$ ✓

□

Def: The ascending central series of G is the following series of subgroups:

$Z^0(G) = \{e\}$, $Z^1(G) = Z(G)$, the center of G

Note that both $Z^0(G), Z^1(G) \triangleleft G$.
Now, let (recursively) $Z^{i+1}(G)$ be the preimage of the center of $G/Z^i(G)$ under the canonical injection π.



By the 4^{th} iso theorem, $Z^{i+1}(G) \triangleleft G$ and $Z^{i+1}(G) \supseteq Z^i(G)$.

Note that $Z^{i+1}(G)/Z^i(G) \cong K$ is abelian.

$\Rightarrow \{e\} = Z^0 \triangleleft \cdots \triangleleft Z^n$ with abelian quotients

Theorem: $\forall$ group G, $Z^m(G) = G$ for some m iff $\gamma_m(G) = \{e\}$. Moreover, in this case $\gamma_i(G) \subseteq Z^{m-i}(G)$ $\forall i \leq m$.

Proof: Suppose $Z^m(G) = G$. We will prove by induction that
$$\gamma_i(G) \subseteq Z^{m-i}(G)$$

* The case $i=0$ is obvious.

* Suppose $\gamma_i(G) \subseteq Z^{m-i}(G)$ and consider

$$\pi : G \to G/Z^{m-i-1}(G)$$

We know that $\pi(Z^{m-i}) = Z(G/Z^{m-i-1})$ ⊛

$\Rightarrow \pi(\gamma_i) \subseteq Z(G/Z^{m-i-1})$ by ind. hyp.

$\Rightarrow \pi(\gamma_{i+1}) = \pi([\gamma_i, G]) \overset{\text{check !}}{=}$

$$= [\pi(\gamma_i), \pi(G)] = \{e\},$$

because $\pi(\gamma_i) \subseteq Z(\pi(G))$ by ⊛

$\therefore \gamma_{i+1} \subseteq \ker(\pi) = Z^{m-i-1}$ ✓

And thus, $\gamma_m \subseteq Z^0 = \{e\} \Rightarrow \gamma_m = \{e\}$.

On the other hand, if $\gamma_m(G) = \{e\}$, we show inductively that $\gamma_i \subseteq Z^{m-i}$.

* The case $i=m$ is again obvious.

* Assume $\gamma_i \subseteq Z^{m-i}$. To show $\gamma_{i-1} \subseteq Z^{m-i+1}$ it is enough to show $\pi(\gamma_{i-1}) \subseteq Z(\pi(G))$, where $\pi : G \to G/Z^{m-i}$ is canonical.

So, we want to show $[\pi(\gamma_{i-1}), \pi(G)] = \{e\}$

but $[\pi(\gamma_{i-1}), \pi(G)] = \pi([\gamma_{i-1}, G]) =$

$= \pi(\gamma_i) = \{e\}$

because $\gamma_i \subseteq Z^{m-i} = \ker(\pi)$ by ind. hyp.

Thus $Z^m(G) \supseteq \gamma_0 = G \Rightarrow Z^m(G) = G$.

□

<u>Example</u>: A nilpotent group is solvable, but not conversely.

S_3 is solvable ($\# S_3 < 60$), but $Z(S_3) = \{e\}$

$\Rightarrow$ Ascending central series does not converge to $G \Rightarrow S_3$ is not nilpotent.

Equivalently $[S_3, S_3] = S_3 \Rightarrow \gamma_0 = \gamma_1 \Rightarrow$
$\Rightarrow \gamma_n \neq \{e\}\ \forall n \Rightarrow$ NOT Nilpotent.

<u>Example</u>: A finite p-group is nilpotent

<u>Proof</u>: If $G \neq \{e\}$, finite p-group, $Z(G) \neq \{e\}$
$\Rightarrow$ either $Z(G) = G$ & we are done,
or $G/Z(G)$ is a non-trivial p-group
and $Z(G/Z(G)) = Z^2(G) \neq Z(G)$

∴ The ascending central series is always increasing $\Rightarrow$ By finiteness, we are done!

□

Example: Let $G_1, \ldots, G_n$ be nilpotent groups.

Then $G_1 \times \ldots \times G_n$ is nilpotent b/c

$$\gamma_m(G_1 \times \ldots \times G_n) = \gamma_m(G_1) \times \ldots \times \gamma_m(G_n)$$

Exercise: A subgroup homo' image of nilpotent groups are also nilpotent.

Fact: It is NOT TRUE that

$\left(H \triangleleft G, \ G/H \text{ both nilpotent} \Longrightarrow G \text{ nilpotent} \right)$

$\hookrightarrow$ Counterexample: $G = S_3$, $H = A_3$ (abelian)

Theorem: A group G is nilpotent iff it is the direct product of its Sylow subgroups.

Remark: This result tells us that nilpotent groups are "very close" to p groups

Lemma: Let G be any finite group, $P < G$ a p-Sylow subgroup.

If $H = N_G(P) = \{ x \in G : xPx^{-1} = P \}$, then

$$N_G(H) = H.$$

Observe that P is a p-Sylow subgroup of H and that $P \triangleleft H \Rightarrow P$ is the unique p-Sylow subgroup of H.

Let $x \in N_G(H)$. It induces an auto' of H by $h \mapsto xhx^{-1}$, as
$xh_1h_2x^{-1} = xh_1x^{-1}xh_2x^{-1}$.

Thus, xPx^{-1} is also a p-Sylow subgroup of H, so by uniqueness, $xPx^{-1} = P$, $\forall x \in N_G(H)$. $\Rightarrow x \in H$.

$$\therefore N_G(H) \subseteq H \subseteq N_G(H) \Rightarrow H = N_G(H)$$

$\square$

<u>Lemma</u>: Let G be a nilpotent group and $H \lneq G$. Then $H \neq N_G(H)$.

<u>Remark</u>: If this property holds $\forall H < G$ of some group G, G must be nilpotent (proof – exercise).

<u>Proof</u>: Consider the descending central series:

$$G = \gamma_0 \triangleright \dots \triangleright \gamma_n = \{e\}$$

As $H \lneq G$, $\exists i$ s.t. $H \not\supseteq \gamma_i$, but $H \supseteq \gamma_{i+1}$. We will now check that $\gamma_i \subseteq N_G(H)$ implying that $H \neq N_G(H)$.

$$[\gamma_i(G), H] \subseteq [\gamma_i(G), G] = \gamma_{i+1} \subseteq H$$

If $x \in \gamma_i$, $y \in H$, $xyx^{-1}y^{-1} \in H \implies$

$$\implies xyx^{-1} \in Hy \overset{y \in H}{=} H \quad \forall y \in H \implies$$

$$\implies \forall x \in \gamma_i,\ xHx^{-1} \subseteq H \implies \gamma_i \subseteq N_G(H) \checkmark$$

$\square$

<u>Proof of Theorem</u>:

[$\Leftarrow$] Known, as any p-group is nilpotent and direct products of nilpotent groups are nilpotent.

[$\Rightarrow$] Assume G is nilpotent and let P be a p-Sylow subgroup.

If $P = G$, we are done; otherwise $P \subsetneq G$, so by lemma, $P \neq N_G(P)$. If $N_G(P) \neq G$,

$$N_G(P) \subsetneq N_G(N_G(P))$$

which contradicts the first lemma. Thus $N_G(P) = G$

$\therefore$ G nilpotent $\implies$ Any p-Sylow subgroup is <u>normal</u> in G.

Write $\# G = p_1^{a_1} \cdots p_r^{a_r}$, $a_i > 0$.

Let P_i be the unique p_i-Sylow subgroup in G.
$P_i \triangleleft G$.

<u>Claim</u>: If $i \neq j$, P_i & P_j commute.

Indeed, if $x \in P_i$, $y \in P_j$,

$$[x,y] = xyx^{-1}y = \begin{cases} \overbrace{(xyx^{-1})}^{\in P_j} y \in P_j \\ x \underbrace{(yx^{-1}y)}_{\in P_i} \in P_i \end{cases}$$

$\Longrightarrow [x,y] \in P_i \cap P_j = \{e\}$ b/c p_i & p_j are primes.

So, define a function $P_1 \times \dots \times P_r \xrightarrow{f} G$
$(x_1, \dots, x_r) \xrightarrow{f} x_1 x_2 \cdots x_r$

As P_i, P_j commute, $x_1 y_1 \cdots x_r y_r = (x_1 \cdots x_r)(y_1 \cdots y_r)$
$\Longrightarrow f$ is a homo.

On each P_i, f is an iso $\Longrightarrow p_i^{a_i} = \# P_i \mid \# \mathrm{Im}(f)$

$\Longrightarrow \# \mathrm{Im}(f) \geq p_1^{a_1} \cdots p_r^{a_r} = \# G \Longrightarrow f$ surjective.

As $\# G = \# \mathrm{Im}(f)$, f is also injective.

$\square$

§ 2.g. Free groups

September-29-10
4:25 PM

Def: Let X be a set. A *free group* on X is a group G with a function

$$X \xrightarrow{i} G,$$

which has the following property: given any group H with a function $X \xrightarrow{j} H$, $\exists!$ homo $f : G \to H$ s.t.

$$\begin{tikzcd} X \arrow[rr, "j"] \arrow[dr, "i"'] & & H \\ & G \arrow[ur, "\exists! f"'] & \end{tikzcd}$$

commutes

Lemma: If G exists, it is unique up to a unique iso.

Proof: (Sketch)

Suppose H with $X \xrightarrow{j} H$ also has the property, then

$$\begin{tikzcd} & G \arrow[d, shift right, "f"'] \\ X \arrow[ur, "i"] \arrow[dr, "j"'] & H \arrow[u, shift right, "g"'] \end{tikzcd}$$

which produces

$$\begin{tikzcd} & G \\ X \arrow[ur, "i"] \arrow[dr, "i"'] & \\ & G \arrow[uu, "g \circ f"'] \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} & G \\ X \arrow[ur, "i"] \arrow[dr, "i"'] & \\ & G \arrow[uu, "\mathbb{1}_G"'] \end{tikzcd}$$

$\therefore$ By uniqueness, $g \circ f = \mathbb{1}_G$, $f \circ g = \mathbb{1}_H$. Done! $\square$

Theorem: There is a free group on X. We will denote the one we construct by $\mathcal{F}(X)$.

Proof: Consider all finite strings

$$\{s_1 \cdots s_N \mid N \geq 0,\ s_i = x \in X \text{ or } x^{-1} \text{ for some } x \in X\}$$

a new formal symbol

These will be called words in the alphabet X. We declare that

1. $xx^{-1} = x^{-1}x = \mathbb{1}$ (another new symbol)
2. $s_1 \cdots s_i s_{i+1} \cdots s_N \sim s_1 \cdots s_i \mathbb{1} s_{i+1} \cdots s_N$

We say that words are equivalent if we can get one from another by applying the two rules above, or their converses. We denote by $[w]$ the equivalence class of w. Set

$$\mathcal{F}(X) = \{[w] : w \text{ is a word in the alphabet } X\}$$

Define multiplication by juxtaposition

$$\begin{aligned} \mathcal{F}(X) \times \mathcal{F}(X) &\longrightarrow \mathcal{F}(X) \\ ([w_1], [w_2]) &\longmapsto [w_1 w_2] \end{aligned}$$

$\hookrightarrow$ Well defined! $\mathcal{F}(X)$ is a group with identity $[\emptyset] = [\mathbb{1}]$ and inverse:

$$([s_1 \cdots s_N]^{-1}) = [s_N^{-1} \cdots s_1^{-1}], \text{ with } (x^{-1})^{-1} := x$$

Define the function $\begin{array}{ccc} X & \xrightarrow{i} & \mathcal{F}(X) \\ x & \longmapsto & [x] \end{array}$

<u>Claim</u>: $(\mathcal{F}(X), i)$ has the univ. property.

$\forall$ group H, $X \xrightarrow{j} H$, define

$$f : \mathcal{F}(X) \longrightarrow H$$

$$f([s_1 \cdots s_N]) \overset{\text{def.}}{=} j(s_1) \cdots j(s_N)$$

* f is well-defined (enough to check for rules (1) & (2)!)

* Clear that
$$\begin{tikzcd} X \arrow[rr, "j"] \arrow[dr, "i"'] & & H \\ & \mathcal{F}(X) \arrow[ur, "f"'] & \end{tikzcd}$$
commutes,

and f is the only possibility as if $g : \mathcal{F}(X) \longrightarrow H$, we must have

$$g([s_1 \cdots s_N]) = g([s_1]) \cdots g([s_N])$$

$\Longrightarrow$ Enough to check for x & x^{-1}:

$$f([x]) = (f \circ i)(x) = j(x) = (g \circ i)(x) = g([x])$$

and the equality $f([x^{-1}]) = g([x^{-1}])$ follows from homo' properties and the observation that $[x^{-1}] = [x]^{-1}$.

$\square$

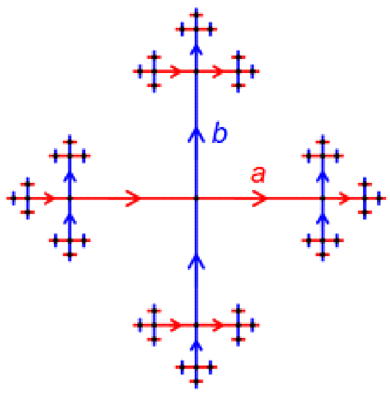
Remarks:

A. We defined $\mathcal{F}(X)$ using an extra symbol $\mathbb{1}$. One can dispense with that & instead of (1) & (2) use

3. $s_1 \cdots s_N \sim s_1 \cdots s_i t t^{-1} s_{i+1} \cdots s_N \sim$
$\sim s_1 \cdots s_i t^{-1} t s_{i+1} \cdots s_N, \quad \forall t \in X.$

B. $X = \{a\} \Rightarrow \mathcal{F}(X) \cong \mathbb{Z} \quad (a \mapsto 1).$

$X = \{a, b\} \Rightarrow \mathcal{F}(X)$ non-abelian and "complicated".



Infinite 4-regular tree T: any word in X gives a path; equivalent paths have the same endpoint.
$\therefore \exists$ bijection between equiv. classes of words and vertices in this tree.

Exercise: Any element $\mathcal{F}(X)$ has a unique representative of minimal length.
$\Rightarrow$ equivalence classes of words $\cong$ geodesics in T.

Also, $\mathcal{F}(X)$ acts as an auto' of T, as given any vertex v & word w, $v * w \longmapsto vw$

$\rightarrow$ T is the universal covering sp. of ∞ and $\mathcal{F}(\{a,b\})$ is its fundamental group.

Def: Let X be a set, a **free abelian group** on X is a group $\mathcal{A}(X)$ and a function $i: X \to \mathcal{A}(X)$, universal for the following diagram

(H is any abelian group)

$$\begin{tikzcd} X \arrow[r, "i"] \arrow[dr, "j"'] & \mathcal{A}(X) \arrow[d, dashed, "\exists! f"] \\ & H \end{tikzcd}$$

$\exists! f: \mathcal{A}(X) \to H$

Properties:

1. If $\mathcal{A}(X)$ exists, it is unique up to a unique iso.

2. $\mathcal{A}(X)$ exists and we can take

$$\mathcal{A}(X) = \{ \ell : X \to \mathbb{Z} \mid \ell(x) \neq 0 \text{ for finitely many } x \in X \}$$

with $X \to \mathcal{A}(X)$, $x \longmapsto \delta_x(y) = \begin{cases} 1, & \text{if } y = x \\ 0, & \text{else.} \end{cases}$

Proof: Exercise.

Proposition: $\mathcal{A}(X) \cong \mathcal{F}(X)^{ab}$

Proof: Enough to check that $\mathcal{F}(X)^{ab}$ has the universal property in Abelian gps

$$\begin{tikzcd} X \arrow[r, "i"] \arrow[dr, "j"'] \arrow[rr, bend left, "\pi \circ i"] & \mathcal{F}(X) \arrow[r, "\pi"] \arrow[d, "\exists! f"] & \mathcal{F}(X)^{ab} \arrow[dl, "f^{ab}"] \\ & H & \end{tikzcd}$$

where $f^{ab}(\bar{s}) = f(s)$
↳ comes from G/G' theory.

Now it only remains to show that f^{ab} is unique. Suppose g^{ab} makes the outer triangle commute. Let $g = g^{ab} \circ \pi$; then

$$g \circ i = g^{ab} \circ (\pi \circ i) = j \Rightarrow g = f \Rightarrow g^{ab} = f^{ab}$$

$\square$

<u>Corollary</u>: $X \xrightarrow{i} \mathcal{F}(X)$ is injective.

<u>Proof</u>: Even the map $X \xrightarrow{i} \mathcal{F}(X) \xrightarrow{\pi} \mathcal{F}(X)^{ab}$ is injective as $x \mapsto \delta_x(y)$ is injective.

$\square$

<u>Corollary</u>: $\mathcal{F}(X) \cong \mathcal{F}(Y) \Leftrightarrow |X| = |Y|$.

<u>Proof</u>: $[\Leftarrow]$ is obvious.

$[\Rightarrow]$ $\mathcal{F}(X) \cong \mathcal{F}(Y) \Rightarrow \mathcal{F}^{ab}_{(X)} \cong \mathcal{F}^{ab}_{(Y)} \Rightarrow \mathcal{A}(X) \cong \mathcal{A}(Y)$

$$\therefore \underbrace{\mathcal{A}(X)/_{2\mathcal{A}(X)}} \cong \mathcal{A}(Y)/_{2\mathcal{A}(Y)}$$

V.sp. over $\mathbb{Z}_2$ with basis $\{\delta_x : x \in X\}$, because $\mathcal{A}(X)/_{2\mathcal{A}(X)} = \{f : X \to \mathbb{Z}_2 \mid \operatorname{supp} f \text{ is finite}\}$.

But by theory of v.sp., all bases have the same cardinality

$$|X| = |\{\delta_x : x \in X\}| = |\{\delta_y : y \in Y\}| = |Y|$$

$\square$

Adjoint functors

September-29-10
5:57 PM

Let C, D be categories, $F: C \to D$, $G: D \to C$ covariant functors.

<u>Def</u>: We say that (F, G) is an adjoint pair, i.e. F is the left adjoint of G and G is the right adjoint of F, if

$\forall A_1, A_2 \in Obj(C)$, $h: A_1 \to A_2$, $B \in Obj(D)$, we have an iso of sets

$$\begin{tikzcd}
Hom_D(F(A_1), B) \arrow[r, phantom, "\overset{f_{A_1,B}}{\cong}"] & Hom_C(A_1, G(B)) \\
Hom_D(F(A_2), B) \arrow[u, "\psi \mapsto \psi \circ F(h)"] \arrow[r, phantom, "\overset{f_{A_2,B}}{\cong}"] & Hom_C(A_2, G(B)) \arrow[u, "\psi \mapsto \psi \circ h"']
\end{tikzcd}$$

And a symmetric requirement for $g: B_1 \to B_2$ in category D.

<u>Remark</u>: There is a similar definition for contracovariant functors.

<u>Example</u>: $C = \underline{Sets}$, $D = \underline{Groups}$

$F: C \to D$, $F(X) = \mathcal{F}(X)$

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[dr, "i"'] & Y \arrow[r, "i"] & \mathcal{F}(Y) \\
& \mathcal{F}(X) \arrow[ur, "\exists!\, F(f)"'] &
\end{tikzcd}$$

Let $G : D \to C$ be the forgetful functor.

$$\mathrm{Hom}_D(\mathcal{F}(X), B) \cong \mathrm{Hom}_C(X, B = G(B))$$

$$f \longmapsto \left(X \xrightarrow{f \circ i} B \right)$$

$$f \longmapsfrom \begin{tikzcd} X \arrow[r, "i"] \arrow[dr, "j"'] & \mathcal{F}(X) \arrow[d, "\exists ! f"] \\ & B \end{tikzcd}$$

One checks properties and finds that (F, G) is an adjoint pair.

Also, if $D =$ <u>Abelian groups</u>, $F(X) = \mathcal{A}(X)$ and G is the forgetful functor $F : D \to C$, (F, G) is an adjoint pair.

Generators and relations

September-29-10
6:19 PM

X – a set, R – a set of words in X.

<u>Def</u>: Let $N(R)$ be the smallest normal subgroup of $\mathcal{F}(X)$ containing R. Then the group

$$\langle X \mid R \rangle = \mathcal{F}(X) / N(R)$$

This group has the following universal property: given any group H and function $f: X \to H$, s.t.

$$f([w]) = \mathbb{1}_H \quad \forall w \in R,$$

$\exists!$ homo' $\langle X \mid R \rangle \xrightarrow{F} H$ s.t. $F(x) = f(x)$ $\forall x \in X$.

<u>Proof</u>: (Sketch).

Uniqueness is clear ($f(x) = F(x)$ $\forall x \in X$). To show existence, first define $\tilde{F}: \mathcal{F}(X) \to H$, then check that $R \subseteq \ker(\tilde{F})$, so by 1st iso' thm,

$$N(R) \subseteq \ker(\tilde{F}) \implies \begin{tikzcd} \mathcal{F}(X) \arrow[rr, "\tilde{F}"] \arrow[dr, "\pi"'] & & H \\ & \langle X \mid R \rangle \arrow[ur, "\exists!\, F"'] & \end{tikzcd}$$

$\square$

<u>Examples</u>:

① $R = \emptyset \implies \langle X \mid R \rangle = \mathcal{F}(X)$

2. $X = \{x\}$, $R = \{x^n\} \Longrightarrow$

$$\Longrightarrow \langle x \mid x^n \rangle \cong \mathbb{Z}_n$$
$$x \longmapsto 1$$

3. $X = \{x, y\}$, $R = \{x^2, y^n, xyxy\} \Longrightarrow$

$$\Longrightarrow \langle x \mid x^2, y^n, xyxy \rangle \cong D_{2n}$$

<u>Proof</u>: * The existence of a surjective homo' is clear. To show injectivity, prove that LHS has $\leq 2n$ elements $\Longrightarrow$
$\Longrightarrow$ by surjectivity, we are done!

* To do so, notice that on the LHS, $\overline{x}\overline{y} = \overline{y^{-1}}\,\overline{x} \Longrightarrow$ any $\overline{w}$ can be written in the form $\overline{x}^{\alpha}\overline{y}^{\beta}$, $\alpha \in \{0, 1\}$, $0 \leq \beta \leq n-1$. □

4. $X = \{x, y\}$, $R = \{[x, y]\}$

$$\langle x, y \mid xyx^{-1}y^{-1} \rangle \cong \mathbb{Z}^2$$

<u>Proof</u>: (Sketch)

Construct a homo' $\begin{cases} x \mapsto (1, 0) \\ y \mapsto (0, 1) \end{cases}$, surjective.
To do so, start from $F(X)$ & use 1^{st} ISO'.
On LHS, $\forall \overline{w} \sim \overline{x}^a \overline{y}^b$ for <u>unique</u> a & b

$$w = x^{\varepsilon_1} y^{\delta_1} \dots x^{\varepsilon_n} y^{\delta_n} \quad \varepsilon_i, \delta_i \in \{\pm 1, 0\} \Longrightarrow \begin{cases} a = \sum \varepsilon_i \\ b = \sum \delta_i \end{cases}$$

$\therefore$ injectivity follows as $\overline{x}^a \overline{y}^b \longmapsto (a, b)$ is injective. □

Free Products

September-27-10
9:55 AM

Let G_1, G_2 be groups.

Def: The *free product* of G_1 and G_2 (if it exists) is the co-product in $\underline{\text{Groups}}$.

We will denote it by $G * G$.

The universal property

$$\begin{tikzcd} G_1 \arrow[r, "\pi_1"] \arrow[dr, bend right, "f_1"'] & G_1 * G_2 \arrow[d, "\exists ! \varphi"] & G_2 \arrow[l, "\pi_2"'] \arrow[dl, bend left, "f_2"] \\ & \mathcal{J} & \end{tikzcd}$$

$G_1 * G_2$

s.t. the diagram commutes

Theorem: The free product exists.

Proof: (Sketch) $G_i \cong \langle X_i \mid R_i \rangle$, where

$X_i = G_i$ as a set, $R_i =$ all words $g_1 \cdots g_N$ s.t. $g_i \in G_i$ & $g_1 \cdots g_N = 1$.

$\Longrightarrow$ Any G_i has a presentation as $\langle X_i \mid R_i \rangle$

Let $G_1 * G_2 = \langle \underbrace{X_1 \sqcup X_2} \mid \underbrace{R_1 \sqcup R_2} \rangle$

disjoint unions of sets

$\pi_1 : G_1 \to G_1 * G_2$ is induced from $X_1 \to X_1 \sqcup X_2$ as follows:

Start with $X_1 \to \mathcal{F}(X_1 \sqcup X_2) \to G_1 * G_2$;

by universal property $\exists\ \mathcal{F}(X_1) \to G_1 * G_2$;

by 1st iso' thm, $\exists\ G_1 \to G_1 * G_2$.

Given $\mathcal{J}$ as above, construct φ.

Use f_1, f_2 to get $\mathcal{F}(X_1 \sqcup X_2) \xrightarrow{\tilde{\varphi}} \mathcal{J}$,

$\tilde{\varphi}([x_i]) = f_i(x_i)$ for $x_i \in X_i$.

Then, check $R_i \xrightarrow{\tilde{\varphi}} \mathbb{1}_{\mathcal{J}}$, b/c if $w \in R_i$,

then $\tilde{\varphi}(w) = f_i(w) = \mathbb{1}_{\mathcal{J}}$ since on G_i,

$w \in R_i \implies w \sim \mathbb{1}_{G_i}$.

Conclude $\varphi : G_1 * G_2 \to \mathcal{J}$ exists, and check that $\varphi \circ \pi_i = f_i$ (N.B. Enough to check it for the generators!).

$\square$

Examples

1. $\mathbb{Z} * \mathbb{Z} \cong \mathcal{F}(\{x,y\})$

b/c $\mathbb{Z} \cong \mathcal{F}(\{x\})$

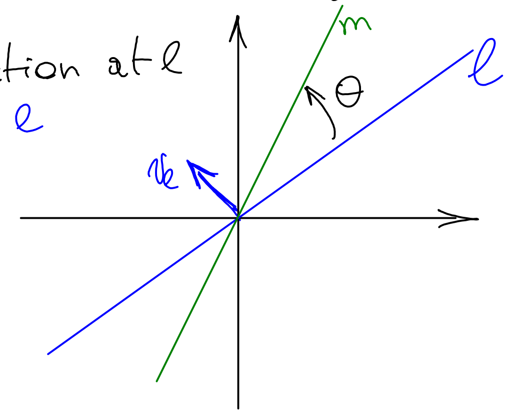
Similarly $*^n \mathbb{Z} \cong \mathcal{F}(\{x_1,\dots,x_n\})$

2. $\mathbb{Z}_2 * \mathbb{Z}_2$ is an infinite group.

Given a line ℓ through the origin of $\mathbb{R}^2$

r_ℓ = reflection at ℓ

v_ℓ is $\perp$ to ℓ



$$r_\ell(w) = w - \frac{2\langle w, v_\ell\rangle}{\|v_\ell\|^2}\cdot v_\ell$$

Check $r_m \circ r_\ell$ = rotation by 2θ counterclockwise.

In particular, if $\frac{2\theta}{2\pi} \notin \mathbb{Q}$, then the rotation by 2θ has infinite order.

$$
\begin{tikzcd}
\langle 1, x \mid x^2 \rangle \cong \mathbb{Z}_2 \arrow[dr] \arrow[ddr, bend right, "f_1"'] & & \mathbb{Z}_2 \cong \langle 1, y \mid y^2 \rangle \arrow[dl] \arrow[ddl, bend left, "f_2"] \\
& \mathbb{Z}_2 * \mathbb{Z}_2 \arrow[d, "\exists! \varphi"'] & \\
& GL_2(\mathbb{R}) &
\end{tikzcd}
$$

$f_1(x) = r_\ell$ $\qquad$ $f_2(y) = r_m$

$\therefore$ $\varphi(xy) = r_m \circ r_\ell$ has ∞-order.

$\Longrightarrow |\mathrm{Im}(\varphi)| = \infty \Longrightarrow \mathbb{Z}_2 * \mathbb{Z}_2$ is infinite.

§ 3.a. Modules

October-12-10
4:48 PM

Let R be an associative ring with 1.

Def: An abelian group $(M,+)$ is a left R-module if we are given an operation

$$R \times M \longrightarrow M, \quad (r,m) \longmapsto r * m = rm$$

such that
* $1m = m \quad \forall m$
* $(r+r')m = rm + r'm$
* $(rr')m = r(r'm)$
* $r(m+m') = rm + rm'$

Def: An R-module homo' $f: M_1 \longrightarrow M_2$, where both M_1 & M_2 are modules over the same ring R, is a map s.t.

* f is a group homo'
* $f(r*m) = r * f(m)$, $r \in R$, $m \in M_1$

The kernel $\ker(f) = \{ m \in M_1 : f(m) = 0_{M_2} \}$ is a submodule of M_1.
$\mathrm{Im}(f) = \{ m \in M_2 : f(n) = m \text{ for some } n \in M_1 \}$ is a submodule of M_2.

The category of all left R-modules is denoted $\underline{R\mathrm{Mod}}$. Analogously, the category of right R-modules is denoted $\underline{\mathrm{Mod}R}$.

<u>Remark</u>: If $\{M_\alpha : \alpha \in \mathcal{A}\} \subseteq \mathrm{Obj}(C)$ for some category C, we can define their product,

$\prod_{\alpha\in\mathcal{A}} M_\alpha \in \mathrm{Obj}(C)$ together with morphisms $\prod_{\alpha\in\mathcal{A}} M_\alpha \xrightarrow{\pi_\alpha} M_\alpha$

universal for the following property:

Given any $D \in \mathrm{Obj}(C)$ with $\{D \xrightarrow{p_\alpha} M_\alpha\}_{\alpha\in\mathcal{A}}$, $\exists!\, f : D \longrightarrow \prod_{\alpha\in\mathcal{A}} M_\alpha$ s.t.

$$\begin{tikzcd} D \arrow[r, "f"] \arrow[dr, "p_\alpha"'] \arrow[dr, phantom, bend left=15, "\circlearrowleft"] & \prod_{\alpha\in\mathcal{A}} M_\alpha \arrow[d, "\pi_\alpha"] \\ & M_\alpha \end{tikzcd}$$

commutes $\forall \alpha \in \mathcal{A}$.

Similarly, the coproduct, $\coprod_{\alpha\in\mathcal{A}} M_\alpha$, is universal for

$$\begin{tikzcd} M_\alpha \arrow[r, "g_\alpha"] \arrow[rr, bend right, "h_\alpha"'] & \coprod_{\alpha\in\mathcal{A}} M_\alpha \arrow[r, "\exists! f"] & D \end{tikzcd}$$

<u>Fact</u>: If products/coproducts exist, they are unique up to a unique iso.

In <u>Sets</u>, $\prod_{\alpha\in\mathcal{A}} M_\alpha$ is the Cartesian product, and $\coprod_{\alpha\in\mathcal{A}} M_\alpha$ is the disjoint union!

<u>Note</u>: Sometimes, the Cartesian product is denoted by $\bigtimes_{\alpha\in\mathcal{A}} M_\alpha$ and the disjoint union by $\biguplus_{\alpha\in\mathcal{A}} M_\alpha$.

Proposition: In **RMod** products & coproducts exist.

Proof: Let $\prod_{\alpha \in A} M_\alpha$ be the R-module with the underlying set $\prod_{\alpha \in A} M_\alpha$, i.e. the Cartesian product of M_α's; and operations:

* $(m_\alpha)_\alpha + (n_\alpha)_\alpha = (m_\alpha + n_\alpha)_\alpha$
* $r(m_\alpha)_\alpha = (r m_\alpha)_\alpha$.

Also set $\pi_{\alpha_0}((m_\alpha)_\alpha) = m_{\alpha_0}$. Now, checking all axioms is a mechanical exercise.

Define $\coprod_{\alpha \in A} M_\alpha$ to be the following submodule of the product module $\prod_{\alpha \in A} M_\alpha$:

$$\coprod_{\alpha \in A} M_\alpha = \left\{ (m_\alpha)_\alpha \in \prod_{\alpha \in A} M_\alpha \;:\; m_\alpha \neq 0 \text{ for finitely many } \alpha \in A \text{ only} \right\}$$

$g : M_{\alpha_0} \longrightarrow \coprod_{\alpha \in A} M_\alpha$, $g(m) = (m_\alpha)_\alpha$, with

$$m_\alpha = \begin{cases} m, & \text{if } \alpha = \alpha_0 \\ 0, & \text{else} \end{cases}.$$

Again, axiom checking is an exercise. $\square$

Examples: (1) If $R = \mathbb{Z}$, **RMod** = **Abelian Groups**

Since $1 * m = m$, $2 * m = (1+1) * m = m + m$, ... abelian group structure determines module structure completely.

② If $R = k$ (a field),

$$\underline{R\mathrm{Mod}} = \underline{k\text{-v.sp.}}$$

③ Let R be any ring.

<u>Def</u>: $I \subseteq R$ is an ideal of R if I is an abelian subgroup s.t. $\forall r \in R, \forall i \in I, ri \in I$.

Then I is an R-module. Moreover, any R-module contained in R is of this form (by definition, basically).

Given $M_1 \subseteq M_2$, R-modules, the abelian group M_2/M_1 is naturally an R-module:

$$r\overline{m} := \overline{rm}, \text{ where } \overline{m} = m + M_1.$$

Let us check that this is well-defined:

$\overline{m_1} = \overline{m_2} \Longrightarrow \exists h \in M_1,\ m_1 = m_2 + h$, then

$$r\overline{m_1} = r\overline{(m_2+h)} = \overline{rm_2 + \underbrace{rh}_{\in M_1}} = \overline{rm_2} = r\overline{m_2} \checkmark$$

The rest is again mechanical.

Isomorphism theorems for rings

October-12-10
5:38 PM

→ We already know that they hold for groups, so in the proof one only needs to show that all group homo's are actually ring homo's.

1. $f : M_1 \to M_2$, R-module homo, $N \subseteq \ker(f)$, then

$$\begin{tikzcd} M_1 \arrow[rr, "f"] \arrow[r, "\pi"'] & M_1/N \arrow[r, "F"'] & M_2 \end{tikzcd}$$

$\exists ! F$ s.t. $F(\bar{m}) = f(m)$

and $\ker(F) = \ker(f)/N$.

2. M_1, M_2 submodules of M,

$$M_1/_{M_1 \cap M_2} \cong (M_1 + M_2)/_{M_2}$$

3. $M_1 \subseteq M_2 \subseteq M_3$ submodules of M,

$$(M_3/M_1)/_{(M_2/M_1)} \cong M_3/_{M_2}$$

4. $f : M_1 \to M_2$ surjective R-module homo

$$\left\{ \begin{matrix} \text{submodules of } M_1 \\ \text{containing } \ker(f) \end{matrix} \right\} \cong \left\{ \begin{matrix} \text{Submodules} \\ \text{of } M_2 \end{matrix} \right\}$$

with the bijection given by $M \longmapsto f(M)$.

Key Example

k - field, V v.sp. over k.

$T : V \longrightarrow V$, a linear map.

Then we can view V as an $\overbrace{k[x]}^{\text{ring of poly. over } k,}$ -module by defining $\forall v \in V$,

$$p(x) \cdot v = p(T)(x)$$

where $p(x) = \sum_{i=0}^{n} a_i x^i \Longrightarrow p(T) = \sum_{i=1}^{n} a_i T^i$.

The verification of axioms rests on the following formulas:

$$* \ (p_1 + p_2)(T) = p_1(T) + p_2(T)$$

$$* \ (p_1 p_2)(T) = p_1(T) \cdot p_2(T)$$

We will now procede to show that this way of viewing vector spaces equipped with linear maps can be made into an equivalence statement between the corresponding categories.

Equivalence of categories

September-29-10
10:16 AM

Let C, D be categories and

$$F_1, F_2 : C \longrightarrow D$$

be covariant functors.

<u>Def</u>: We say that F_1 is naturally equivalent to F_2 if $\forall A \in Obj(C)$ we are given an iso

$$F_1(A) \xrightarrow{\varphi_A} F_2(A)$$

such that $\forall f : A \to A'$ we have a commutative diagram

$$\begin{tikzcd} F_1(A) \arrow[r, "\varphi_A"] \arrow[d, "F_1(f)"'] \arrow[dr, phantom, "\circlearrowleft"] & F_2(A) \arrow[d, "F_2(f)"] \\ F_1(A') \arrow[r, "\varphi_{A'}"'] & F_2(A') \end{tikzcd}$$

<u>Remark</u>: The only change necessary to make this definition work for contracovariant functors is to use arrows going up ($\uparrow$) in the diagram.

<u>Notation</u>: If F_1 is naturally equivalent to F_2, we often write $F_1 \cong F_2$

Def: Two categories C, D are called *equivalent* (resp. *anti-equivalent*) if $\exists$ covariant (resp. contracovariant) functors

$$F : C \longrightarrow D, \quad G : D \longrightarrow C$$

such that $F \circ G \cong \mathbb{1}_D$, $G \circ F \cong \mathbb{1}_C$

Equivalently, $\forall A \in Obj(D)$, $\exists$ isò φ_A s.t.

$$\begin{tikzcd} \mathbb{1}_D(A) := A \arrow[r, "\varphi_A"] \arrow[d, "f"'] \arrow[dr, phantom, "\circlearrowleft"] & F \circ G(A) \arrow[d, "F\circ G(f)"] \\ \mathbb{1}_D(A) := A' \arrow[r, "\varphi_{A'}"] & F \circ G \end{tikzcd}$$

and similarly for $G \circ F$.

__Example__: Let $C = D =$ __Finite dimensional k-v.sp.__

$F : C \to C$, $F(V) = V^* = Hom_k(V, k)$
$F(T : V \to W) = T^* : W^* \to V^*$, $(T^* \psi) v = \psi(Tv)$

__Claim__: (F, F) Gives an auto-anti-equivalence, usually called *duality*

$\hookrightarrow$ We need to show that

$$F \circ F \cong \mathbb{1}_C$$

To do so, $\forall V \in \mathrm{Obj}(\mathcal{C})$, define $V \xrightarrow{\varphi_V} (V^*)^*$

$\forall x \in V$, $\varphi_V(x)$ is a linear functional on V^*, so to define it, we must give its value on any $\psi \in V^*$. Thus,

$$\big(\varphi_V(x)\big)(\psi) = \psi(x)$$

One checks that this is indeed a linear functional on V^* and that the map $\varphi_V : V \to V^{**}$ is itself linear.

- φ_V is <u>injective</u> : for suppose $\varphi_V(x) = 0$ for some $x \neq 0$. We complete $\{x\}$ to a basis $\{x = v_1, \dots, v_n\}$ and set

$$\psi : V \to k, \ \psi\Big(\sum_i \alpha_i v_i\Big) = \alpha_1 \Rightarrow \psi(x) = 1.$$

$$\Rightarrow \big(\varphi_V(x)\big)\psi = \psi(x) = 1 \Rightarrow \varphi_V(x) \neq 0.$$

- Since $\dim(V) = \dim(V^*) = \dim(V^{**})$, φ_V is also <u>surjective</u>. ✓

- We now need to check that

$$\begin{array}{ccc} V & \xrightarrow{\varphi_V} & V^{**} \\ T\downarrow & & \downarrow T^{**} \\ W & \xrightarrow{\varphi_W} & W^{**} \end{array}$$ commutes.

That is $T^{**} \circ \varphi_V = \varphi_W \circ T$.

Let $x \in V$, as $(T^{**} \circ \varphi_V)(x) \in W^{**}$, we need to check that it has the same value as $(\varphi_W \circ T)(x)$ on any $\psi \in W^*$:

$$\left[T^{**}(\varphi_V(x))\right](\psi) = [\varphi_V(x)](T^*\psi) =$$
$$= (T^*\psi)(x) = \psi(Tx)$$

On the other hand $[\varphi_W(Tx)]\psi = \psi(Tx)$. $\square$

<u>Proposition</u>: Let k be a field, and C a category with $Obj(C) = \{(V,T) : V$ is a k-v.sp. and $T: V \to V$ a linear map$\}$,

and morphisms $L: (V_1, T_1) \to (V_2, T_2)$, where $L: V_1 \to V_2$ is a linear map such that

$$L \circ T_1 = T_2 \circ L$$

If $D = \underline{k[x]\,Mod}$, then C is equivalent to D.

<u>Proof</u>: We have already seen that, given a pair (V,T), we can make V into a $k[x]$-module by defining $\forall v \in V$,

$$p(x) \cdot v = (p(T))(v)$$

In particular $x \cdot v = Tv$.

Any $L : (V_1, T_1) \to (V_2, T_2)$ becomes a $k[x]$-module homo' as

$$L(p(x) \cdot v) = \big(L \circ p(T_1)\big) v =$$
$$= \big(p(T_2) \circ L\big) v = p(T_2) \cdot Lv \checkmark$$

Conversely, if V is any $k[x]$-module, define $T : V \to V$ by $Tv := x \cdot v$, $\forall v \in V$.

WRONG ?? As k is a subring of $k[x]$, V is also a k-module. Thus V is a k-v.sp.
$\Rightarrow (V, T) \in \mathrm{Obj}(C)$.

Let $L : V_1 \to V_2$ be a $k[x]$-module homo'.

$$(L \circ T_1) v = L(x \cdot v) = x\, L(v) = (T_2 \circ L) v \checkmark$$

__Remark__: If we call the two functors defined above $F : C \to D$ & $G : D \to C$, we see that

$$F \circ G = \mathbb{1}_D \ , \quad G \circ F = \mathbb{1}_C$$

equality, not equivalence!

Later, we will apply results from the theory of modules to k-vsp. with linear maps to get Jordan canonical form and much more.

§ 3.b Further concepts in the theory of modules

October-12-10
11:08 PM

Let M be a left R-module, and I a left ideal of R.

Def: Set

$$IM = \left\{ \sum_{\alpha=1}^{n} i_\alpha m_\alpha : i_\alpha \in I, m_\alpha \in M \right\}$$

This is clearly a submodule of M.

Def: Let $N \subseteq M$ be a submodule, define the annihilator of N by

$$\mathrm{Ann}(N) = \{ r \in R : rn = 0 \ \forall n \in N \}$$

This is a two sided ideal of R, and

N is an $R/\mathrm{Ann}(N)$ - module with multiplication given by $\bar{r} \cdot n = rn$

N.B. $R/\mathrm{Ann}(N)$ is a ring, because $\mathrm{Ann}(R)$ is a two-sided ideal of R.

Similarly, if J is any two-sided ideal of R, contained in $\mathrm{Ann}(N)$, then N is also an R/J-module.

Thus, if I is a two sided ideal of R, M/IM is an R/I-module.

Def: M is said to be *finitely generated* if $\exists x_1, \dots, x_n \in M$ s.t. $\forall y \in M$,

$$y = \sum_{i=1}^{n} r_i x_i \quad \text{for some } r_i \in R.$$

N.B. The $\{r_i\}$ need not be unique!

Equivalently, M is finitely generated if $\exists$ a surjective homo'

$$f : R^n \longrightarrow M$$

In fact, setting $f(r_1, \dots, r_n) = \sum_{i=1}^{n} r_i x_i$, proves $[\Longrightarrow]$, while taking

$$x_i = f(0, \dots, 0, \overset{i^{\text{th}} \text{ coordinate}}{1}, 0, \dots, 0) =: f(e_i)$$

proves $[\Longleftarrow]$.

Examples: ① $R = k$, a field, then M is fin. gen. $\Longleftrightarrow$ M is fin. dim'l.

② The ideal $(2, \sqrt{-6})$ of the ring $\mathbb{Z}[\sqrt{-6}]$ is generated by 2 & $\sqrt{-6}$, i.e.

$$(2, \sqrt{-6}) = 2 \cdot \mathbb{Z}[\sqrt{-6}] + \sqrt{-6}\, \mathbb{Z}[\sqrt{-6}],$$
$$\mathbb{Z}[\sqrt{-6}] = \{ a + b\sqrt{-6} : a, b \in \mathbb{Z} \}.$$

But no uniqueness as $6 = 2 \cdot 3 = (\sqrt{-6})(-\sqrt{-6})$

$\hookrightarrow$ Exercise: $(2, \sqrt{-6})$ is not a principal ideal.

Def: An R-module M is said to be cyclic, if it can be generated by a single element, i.e. $\exists\, x \in M$ s.t

$$M = \langle x \rangle = Rx$$

Equivalently, $\exists$ surj. homo of R-modules

$$R \twoheadrightarrow M \quad , \quad r \mapsto rx .$$

Then $\mathrm{Ann}(x) = \{ r \in R : rx = 0 \}$ is the kernel of this homo $\Rightarrow$ $\mathrm{Ann}(x)$ is a left R-submodule of R $\Rightarrow$ $\mathrm{Ann}(x)$ is a left ideal.

$$\therefore M \cong R/\mathrm{Ann}(x)$$

Conversely, $\forall$ left ideal I of R, $M := R/I$ is a left R-module, which is cyclic as

$$R \twoheadrightarrow R/I \quad (\text{canonical surjection})$$

$\Rightarrow$ M is generated by 1.

Example: k - field, V - finite dimensional k-v.sp. $T : V \to V$, a linear map.

We know that $(V, T) \longleftrightarrow k[x]$-module.

$\therefore$ What does it mean for (V,T) to yield a cyclic $k[x]$-module?

Say $\dim(V) = n$, then

Cyclic $\iff \exists x \in V$ s.t. $\forall y \in V$, $y = p(T)x$ for some $p \in k[x]$.

$\iff \{x, Tx, T^2x, \dots, T^{n-1}x\}$ is spanning.

Let $m = \deg(\text{min. poly. of } T)$, then $m \leq n$, and

$\{x, Tx, \dots, T^{m-1}x\}$ is already spanning

$\therefore$ Cyclic $\implies$ $m = n$, that is the equivalence min. poly. $\cong$ char. poly.

<u>Question</u>: Is $\Leftarrow$ also true?

$\hookrightarrow$ We will come back to that.

Free modules

October-04-10
9:51 AM

Let X be a set.

Def: A free R-module on X is a module M, together with a function

$$X \xrightarrow{i} M$$

s.t. given any R-module N with a function

$$X \xrightarrow{j} N$$

$\exists!$ R-module homo $f: M \to N$ s.t.

$$\begin{tikzcd} X \arrow[r, "i"] \arrow[dr, "j"'] & M \arrow[d, "f"] \\ & N \end{tikzcd}$$

commutes.

Fact: As usual, if a free R-module exists, it is unique up to a unique iso.

Lemma: Such M exists.

Proof: Let $M = \bigoplus_{x \in X} R_x$, $R_x = R$ $\forall x$.

and let $i: X \to M$, $i(x) = e_x$

$$e_x \text{ "="} (0, \ldots, 0, \underset{\uparrow\, x^{th} \text{ place}}{1}, 0, \ldots, 0)$$

Given j, define

$$f\left((m_x)_{x\in X}\right) = f\left(\sum_{\{x : m_x \neq 0\}} m_x \cdot e_x\right) =$$

$$= \sum_{x\in X} m_x \cdot j(x)$$

<u>Note</u>: $X \underset{\text{(injects)}}{\hookrightarrow} M$

<u>Proposition</u>: M is free on a set $X \subseteq M$, iff $\forall m \in M$ has a <u>unique</u> expression as $\sum_{x\in X} r_x \cdot x$, $r_x \in R$, $r_x \neq 0$ for finitely many x only

<u>Proof</u>: If M is free, then

$$M \cong \bigoplus_{x\in X} R$$

generated by finite lin. comb. of $\Sigma r_i x_i$

$$X \ni x \longmapsto e_x$$

On the LHS, $(r_x)_{x\in X} = \sum_{x\in X} r_x e_x$ uniquely.

Conversely, define $\bigoplus R \longrightarrow M$ by

$$(r_x)_x \longmapsto \sum_x r_x \cdot x$$

↳ bijective by assumption. $\square$

Theorem: Let R be a non-zero commutative ring, M a free module on X and N a free module on Y. Then

$$M \cong N \iff |X| = |Y|$$

Proof:

$[\Longleftarrow]$ is clear. If $f: X \to Y$ bijective

$$\bigoplus_{x \in X} R \cong \bigoplus_{y \in Y} R \quad \text{by} \quad e_x \longmapsto e_{f(x)}$$

We will come back to $[\Longrightarrow]$ later.

$\square$

Def: S a set. We say that S is a poset (Partially Ordered set) if we are given a relation $x \leq y$ on elements of S s.t.

1. $x \leq x \quad \forall x \in S$
2. $x \leq y,\ y \leq z \implies x \leq z$

N.B. We do <u>not</u> require that $\forall x, y \in S$, either $x \leq y$ or $y \leq x$.

Def: A chain in S is a subset $C \subseteq S$ s.t. $\forall x, y \in C$, either $x \leq y$ or $y \leq x$.

Examples:

* $\mathbb{R}$ & $[0,1]$

* The non-zero ideals of $\mathbb{Z}$ by defining $I \leq J$ if $I \subseteq J$ (if $I = (i)$, $J = (j)$, then $I \leq J$ iff $i \mid j$).

* V k-v.sp., S is a set of lin. indep. subsets X of V, with

$$X \leq Y \iff X \subseteq Y.$$

Def: We say that a chain C is bounded, if $\exists s \in S$ s.t. $x \leq s$ $\forall x \in C$.

Zorn's Lemma: If S is a poset s.t. every chain is bounded, then S has a maximal element s^*, i.e. $\exists s^* \in S$ s.t. $(s \geq s^* \implies s = s^*)$.

Rmk: Zorn's lemma $\Longleftrightarrow$ Axiom of choice.

Axiom of choice: If $\{X_\alpha : \alpha \in A\}$ is a collection of non-empty sets, then

$$\prod_{\alpha \in A} X_\alpha \neq \emptyset$$

($\exists (x_\alpha)_{\alpha \in A}$ in this product means we have chosen $x_\alpha \in X_\alpha$, $\forall \alpha \in A$).

Classical applications (Exercises)

Proposition: Every v.sp. V has a basis.

$\hookrightarrow$ Take S to be the set of lin. indep. subsets of V under inclusion.

Proposition: Every non-zero ring R has a maximal proper left ideal

$\hookrightarrow$ Take S to be the set of proper left ideals.

Proposition: If R is a commutative ring,
M is a free R-module on X,
N is — " — " — on Y.
Then $M \cong N \Longleftrightarrow \#X = \#Y$.

$\hookrightarrow$ Take I to be the max'l ideal, consider $M/IM \cong N/IN$ over R/I.

Torsion

October-13-10
9:49 AM

$\longrightarrow$ From now on, R is an integral domain, i.e. a commutative, non-zero ring s.t.
$xy = 0 \Rightarrow (x=0$ or $y=0)$

<u>Def</u>: Let M be an R-module, set

$$\mathrm{Tors}(M) = \{m \in M \mid \exists r \neq 0 \text{ with } rm = 0\}$$

$\mathrm{Tors}(M)$ is a submodule of M.

<u>Examples</u>:

- $R = \mathbb{Z}$, M = ab. group., then

  $\mathrm{Tors}(M) = \{\text{elements of finite order}\}$

- $R = \mathbb{F}[x]$, $M \longleftrightarrow (V.sp. \text{ with } T : M \to M)$

Assume M is finite dimensional, then
$\mathrm{Tors}(M) = M$, because $f(x) \cdot m \overset{def.}{=} (f(T))(v)$
which is 0 if f is the min. poly. of T.

- M = free R-module, then

  $\mathrm{Tors}(M) = \{0\}$, b/c $M \cong R^N$ & R is an integral domain!

$\hookrightarrow$ Converse is <u>not</u> true!

- $\mathrm{Tors}\left(M/\mathrm{Tors}(M)\right) = \{0\}$

↳ Proof: Exercise.

———— ∘ ————

Rank

Def: $\{x_1, \dots, x_n\}$ in M are linearly dependent if $\exists r_i \in R$, not all 0 s.t.

$$r_1 x_1 + \dots + r_n x_n = 0$$

Def: A subset $S \subseteq M$ is called linearly independent if every finite subset of S is not linearly dependent.

Def: The rank of M is the maximal size of a lin. indep. set.

Proposition: $\mathrm{rank}(M) = \mathrm{rank}\left(M/\mathrm{Tors}(M)\right)$

Proof: Suppose $\{x_1, \dots, x_n\} \subseteq M$ is lin. indep. Let $\{\overline{x_1}, \dots, \overline{x_n}\} \subseteq M/\mathrm{Tors}(M)$ be the image of $\{x_1, \dots, x_n\}$ under the canonical map.

If $\exists r_i$ s.t. $r_1 \overline{x_1} + \dots + r_n \overline{x_n} = 0$, then

$$r_1 x_1 + \dots + r_n x_n = m \in \mathrm{Tors}(M) \implies \exists r \neq 0,\ rm = 0$$

$\implies (rr_1)x_1 + \dots + (rr_n)x_n = 0 \implies rr_i = 0\ \forall i \implies$

$\implies$ By int. dom. property, $r_i = 0\ \forall i$. ✓

So, we got $\operatorname{rank}(M) \leq \operatorname{rank}(M/\operatorname{Tors}(M))$.

Now let $y_1, \dots, y_n \in M/\operatorname{Tors}(M)$ lin. indep., say $y_i = \overline{x_i}$.

Then $r_1 x_1 + \dots + r_n x_n = 0$ (in M) $\Longrightarrow$

$\Longrightarrow r_1 y_1 + \dots + r_n y_n = 0$ in $(M/\operatorname{Tors}(M))$

$\Longrightarrow r_i = 0 \ \forall i \longrightarrow \{x_1, \dots, x_n\}$ is lin. indep.

$\Longrightarrow \operatorname{rank}(M) = \operatorname{rank}(M/\operatorname{Tors}(M))$

$\square$

<u>Proposition</u>: R^n has rank n.

<u>Proof</u>: Set $e_i = (0, \dots, 0, \overset{i^{th}\text{ position}}{1}, 0, \dots, 0)$, then

$\{e_1, \dots, e_n\}$ is lin. indep. $\Longrightarrow \operatorname{rank} \geq n$.

We'll show later that $R \subseteq F$ (a field), called the fraction field of R, s.t.

$\forall f \in F, \exists r \neq 0, r \in R$, s.t. $rf \in R$

$\Longrightarrow R^n \subseteq F^n$.

Let $\{x_1, \dots, x_m\}$ be lin. indep. set in R^n.

<u>Claim</u> : $\{x_1,\dots,x_m\}$ is lin. indep. in F^n over F.

↳ Say $\sum f_i x_i = 0$, $f_i \in F$. Then,

for each i, $\exists r_i \neq 0$ s.t. $r_i f_i \in R$, thus,

multiplying the above by $(r_1 \cdots r_n) =: r$,

we have that $\sum (r f_i) x_i = 0$ in R^n

$\Rightarrow r f_i = 0 \ \forall i \xrightarrow{b/c\ F\text{-field}} f_i = 0 \ \forall i$.

$\therefore$ By v.sp. theory, $m \leq n$.

$\square$

<u>Proposition</u>: Any two maximal lin. indep. sets in M have the same cardinality.

<u>Proof</u>: Only for the case when one of them is finite.

Say $\{y_1,\dots,y_n\}$ and $\{x_1,\dots,x_m\}$ are maximal lin. indep. sets in M. Show $m \leq n$.

Check:

- $\langle y_1,\dots,y_n\rangle = Ry_1 + \dots + Ry_n$ is a free R-mod. of rank n.

Set $N = \langle y_1,\dots,y_n\rangle$, then

- M/N is torsion (i.e. $M/N = \mathrm{Tors}(M/N)$)

  $\hookrightarrow$ If not, $\{y_1, \dots, y_n\}$ is not maximal.

- $\exists r \in R$, $r \neq 0$ s.t. $\{rx_1, \dots, rx_m\} \subseteq N$ is <u>still</u> lin. indep.

- As $N \cong R^n$, $\mathrm{rank}(N) = n \Rightarrow m \leq n$

  Done!

$\square$

§ 3.c Modules over PIDs

October-15-10
9:37 AM

R is a PID ($\underbrace{\text{principal}}$ $\underbrace{\text{ideal domain}}$)

Any ideal is of the form $Ra = aR = (a) = \langle a \rangle$

$R \neq 0$
$xy = 0 \Rightarrow x = 0$ or $y = 0$
commutative

e.g. $\mathbb{Z}$, $\mathbb{F}$, $\mathbb{F}[x]$, but

$\mathbb{C}[x,y]$ is ID, but not PID b/c (x,y) is not principal.

$\mathbb{Z}[\sqrt{-6}]$ is ID, but not PID, b/c $(2, \sqrt{-6})$ is not principal

In a PID, we can talk about gcd's:

$a \mid b$ if $b = a \cdot c$ for some c

$d = \gcd(a,b)$ if $d \mid a$, $d \mid b$ and
$(d' \mid a \,\&\, d' \mid b \Rightarrow d' \mid d)$

Such d is uniquely determined, <u>if</u> it exists, up to a unit.

If R is a PID, $a, b \in R$, let $d \in R$ be s.t. $\langle d \rangle = \langle a, b \rangle = Ra + Rb$.
Then $d = \gcd(a,b)$.

Check!

Theorem (Elementary divisors theorem)

Let R be a PID, M a free R-module of rank m, $N \subseteq M$ a submodule. Then

1. N is free of rank n.
2. $\exists$ basis $y_1, \dots, y_m$ of M and $0 \neq a_1 | a_2 | \dots | a_n$ in R, s.t.

$$a_1 y_1, \dots, a_n y_n \text{ is a basis for } N.$$

Corollary: L, M free fin. gen. R-modules

$$f : L \to M \text{ homo'}$$

Then $\exists$ bases $\{y_1, \dots, y_n\}$ of M, $\{z_1, \dots, z_t\}$ of L such that in these bases f is represented by

$$\operatorname{diag}(a_1, \dots, a_m, 0, \dots, 0) \quad 0 \neq a_1 | \dots | a_m$$

Proof of Corollary: Let $N = f(L)$ submodule of M. Choose

$$\{y_1, \dots, y_n\} \subseteq M$$

as in the theorem, s.t. $\{a_1 y_1, \dots, a_m y_m\}$ is a basis of N. Let $z_1, \dots, z_m \in L$ be s.t.

$$f(z_i) = a_i y_i$$

Let $\{z_{m+1}, \dots, z_t\}$ be a basis for $\ker(f)$ (using Theorem again).

<u>Claim</u>: $\{z_1, \dots, z_t\}$ is a basis for L.

Indeed, if $\ell \in L$, $f(\ell) = \sum_1^m r_i a_i y_i =$

$= \sum_1^m r_i f(z_i)$

So, $\underbrace{\ell - \sum_1^m r_i z_i}_{\in \ker(f)} = \sum_{m+1}^t r_i z_i \quad r_i \in R$.

$\Rightarrow \{z_i\}_1^t$ spans L ✓

Suppose $\sum_{i=1}^t r_i z_i = 0 \xRightarrow{\text{apply } f} \sum_{i=1}^m r_i f(z_i) = 0$

$\Rightarrow \sum_1^m r_i a_i y_i = 0 \xrightarrow{\{y_i\} \text{ is a basis}} r_i a_i = 0 \ \forall i \xrightarrow{\text{PID}} r_i = 0 \ \forall i.$

Thus $\sum_{m+1}^t r_i z_i = 0 \Longrightarrow r_i = 0 \ \forall i$ b/c $\{z_i\}_{m+1}^t$ is a basis for $\ker(f)$

$\square$

Before proceding to the proof of elementary divisors theorem, let us prove a lemma.

<u>Lemma</u>: Under the conditions of EDT, if $N \neq 0$, $\exists\, \varphi : M \to R$ homo', $0 \neq a_1 \in R$ and $y \in N$ s.t.

$\varphi(y) = a_1$ and for every $\psi : M \to R$ homo',

$$a_1 \mid \psi(y)$$

Moreover, $\psi(N) = Ra_1$.

<u>Proof</u>: Let $\Sigma = \{\varphi(N) \mid \varphi \in \mathrm{Hom}_R(M,R)\}$.

Σ is a collection of ideals of R and non-empty as $\varphi \equiv 0 \Rightarrow (0) \in \Sigma$.

<u>Claim</u>: Σ has a maximal element

Suppose not, then $\exists\, \varphi_1, \varphi_2, \dots$ s.t.

$$\begin{array}{ccccccc} \varphi_1(N) & \subsetneqq & \varphi_2(N) & \subsetneqq & \cdots \subsetneqq & \varphi_i(N) & \subsetneqq \cdots \\ \text{PID}\,\| & & \text{PID}\,\| & & & \text{PID}\,\| & \\ (a_{\varphi_1}) & \subsetneqq & (a_{\varphi_2}) & \subsetneqq & \cdots \subsetneqq & (a_{\varphi_i}) & \end{array}$$

But $\bigcup_{i=1}^{\infty} (a_{\varphi_i})$ is an ideal $\Rightarrow \bigcup_{i=1}^{\infty}(a_{\varphi_i}) = (a_\infty)$ for some $a_\infty \in R$. Also, $a_\infty \in (a_{\varphi_i})$ for some i.

$\Rightarrow (a_{\varphi_i}) = (a_{\varphi_{i+1}}) = \dots$ Contradiction!

Choose $M \overset{g}{\cong} R^n \xrightarrow{P_i} R$, P_i i^{th} projection.

Then $p_i \circ g$ is non-zero on N for some i.

$\Longrightarrow \Sigma$ has non-zero elements.

Let φ be s.t. $\varphi(N) =: (a_1)$ is a max'l element of Σ. Then $a_1 \neq 0$.

Let $y \in N$ be s.t. $\varphi(y) = a_1$, clearly

$$\varphi(N) = Ra_1.$$

Let $\psi \in \mathrm{Hom}_R(M,R)$, let $a_2 = \psi(y)$ and

$d = \gcd(a_1, a_2) = r_1 a_1 + r_2 a_2$ for some $r_i \in R$.

$(d) = (a_1, a_2) = Ra_1 + Ra_2$.

The map $\tilde{\varphi} = r_1\varphi + r_2\psi \in \mathrm{Hom}_R(M,R)$.

and $(r_1\varphi + r_2\psi)(y) = d \mid a_1 \Longrightarrow$

$\Longrightarrow \tilde{\varphi}(N) \supseteq \varphi(N) \overset{\text{max'l}}{\Longrightarrow} \tilde{\varphi}(N) = \varphi(N)$

$\Longrightarrow a_1 \mid d \Longrightarrow a_1 \mid a_2$

$\square$

<u>Remark</u>: In particular, $a_1 \mid (p_i \circ g)(y)\ \forall i$.

$\Rightarrow y = a_1 y_1$ for some $y_1 \in M$.

Therefore $a_1(\varphi(y_1) - 1) = \varphi(y) - a_1 = 0$

$$\Rightarrow \varphi(y_1) = 1.$$

<u>Lemma</u>: With notation from previous lemma,

1. $M = \langle y_1 \rangle \oplus \ker \varphi$
2. $N = \langle a_1 y_1 \rangle \oplus (\ker \varphi \cap N)$

<u>Proof</u>: To prove (1), let $x \in M$, $\varphi(x) = \alpha \in R \Rightarrow$

$\Rightarrow x - \alpha y_1 \in \ker(\varphi) \Rightarrow M = \langle y_1 \rangle + \ker(\varphi)$

Let $x \in \langle y_1 \rangle \cap \ker(\varphi)$, say $x = \alpha y_1$, then

$\varphi(x) = \alpha = 0$, b/c $x \in \ker(\varphi)$

$\Rightarrow x = 0$

$\therefore M = \langle y_1 \rangle \oplus \ker(\varphi)$ ✓

Proof of (2) is similar $\Rightarrow$ Exercise.

$\square$

Proof of Elementary divisors theorem:

We prove part (1) by induction on

$$n := \text{rank}(N)$$

* If $m=0$, N is torsion, but M is torsion-free $\Rightarrow N = \{0\}$. ✓

* Consider $N \cap \ker\varphi$. If it has rank ℓ, then $\underbrace{\langle a_1 y_1 \rangle}_{\text{free of rank 1}} \oplus (N \cap \ker\varphi)$ has rank $\geq \ell+1$

Thus, $\ell \leq n-1$, so by induction hyp.,

$N \cap \ker\varphi$ is free of rank $\ell \Rightarrow$
$\Rightarrow N \cong R^{\ell+1}$ ✓ ($\Rightarrow \ell = n-1$, in fact)

We now prove part (2), by induction on

$$m := \text{rank}(M)$$

First, WLOG $N \neq \{0\}$, then we have

$$\underbrace{N \cap \ker\varphi}_{\text{free of rank } n-1} \subseteq \underbrace{\ker\varphi}_{\text{By (1), free of rank } m-1}$$

By induction, $\exists$ basis $\{y_2, \dots, y_m\}$ for $\ker(\varphi)$, and

$$a_2 \mid a_3 \mid \dots \mid a_n, \quad a_i \neq 0$$

such that $\{a_2y_2, \dots, a_ny_n\}$ is a basis for $N \cap \ker \varphi$.

$\therefore$ We already have that

$$\left[\begin{array}{l} \{y_1, \dots, y_m\} \text{ is a basis for } M \\ \{a_1y_1, \dots, a_ny_n\} \text{ is a basis for } N \end{array}\right.$$

$\longrightarrow$ The only missing information is that $a_1 | a_2$

To see this, apply the first lemma to

$$\psi : M \longrightarrow R, \quad \psi\left(\sum b_i y_i\right) = b_1 + b_2$$

N.B. $\psi(\underbrace{a_1y_1}_{=y}) = a_1 \Rightarrow \psi(N) \supseteq (a_1)$

$\xRightarrow{\text{by Lemma}} \psi(N) = (a_1) \Rightarrow a_1 \mid \psi(\underbrace{a_2y_2}_{\in N}) = a_2$ ✓

$\square$

<u>Theorem</u>: Structure theorem (in invariant factors form) for modules over PID.

R – PID, M – f.g. R–module. Then

① $M \cong R^r \oplus R/(a_1) \oplus \dots \oplus R/(a_m)$

for some $r \geq 0$, $0 \neq a_1 | a_2 | \dots | a_m$,

and $\operatorname{rank}(M) = r$.

(2) M is torsion-free $\iff$ M is free.

In fact $\mathrm{Tors}(M) = R/(a_1) \oplus \cdots \oplus R/(a_m)$ with $\{a_i\}$ as in (1).

Proof: Let $x_1, \ldots, x_n$ be generators of M. The map $R^n \longrightarrow M$, $(r_1, \ldots, r_n) \longrightarrow \sum r_i x_i$ is surjective. Let N denote its kernel.

By previous theorem, $\exists$ basis $\{y_1, \ldots, y_n\}$ of R^n $a_i \neq 0$, $a_1 | \cdots | a_m$ s.t.

$\{a_1 y_1, \ldots, a_m y_m\}$ is a basis for N

$$M \cong R^n/N \cong \left(Ry_1/Ra_1y_1\right) \oplus \cdots \oplus \left(Ry_m/Ra_my_m\right) \oplus$$
$$\oplus Ry_{m+1} \oplus \cdots \oplus Ry_n.$$
$$\cong R^r \oplus \left(\bigoplus_{i=1}^{m} R/(a_i)\right), \quad r = n-m.$$

Since $a_m \neq 0$ and kills? $\oplus R/(a_i)$ and as

$$\mathrm{Tors}(A \oplus B) = \mathrm{Tors}(A) \oplus \mathrm{Tors}(B),$$

$$\mathrm{Tors}(M) = \bigoplus_{i=1}^{m} R/(a_i).$$

Then, using $\mathrm{rank}(M) = \mathrm{rank}(M/\mathrm{Tors}(M))$, the result follows.

$\square$

Remark : Uniqueness.

If a_i is a unit, then $R/(a_i) = R/R \simeq \{0\}$, so we may as well assume that each a_i is not a unit.

Then the ideals $(a_1), \dots, (a_m)$ are unique (and so is r), i.e. $\{a_i\}$ are unique up to units.

Recall : (A PID is a UFD)

If R is an ID, p is prime if

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b,$$

p is irreducible if $p = ab \Rightarrow a$ or b is a unit.

Also, p - prime $\Rightarrow$ p - irreducible, and if R is a PID, irreducible $\Rightarrow$ prime, b/c $p \mid ab$, $p \nmid a \Rightarrow \gcd(p,a) = 1$. Then $1 = xp + ya$ for some $x, y \in R \Rightarrow$
$\Rightarrow b = p \cdot xb + (ab)y \Rightarrow p \mid b$.

Theorem : R - PID, then $\forall\, 0 \neq a \in R$, if a is not a unit, $\exists!$ primes $p_i \neq p_j$, positive integers α_i s.t.

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

Also, the Chinese remainder theorem holds:

$$R/(a) \cong \bigoplus_{i=1}^{r} R/(p_i^{\alpha_i}) .$$

Hence, applying these results to M

$$M \cong R^r \oplus \left(\bigoplus_{i=1}^{m} R/(a_i) \right) \Longrightarrow$$

$$\Longrightarrow M \cong R^r \oplus \left(\bigoplus_{i=1}^{T} R/(p_i^{\alpha_i}) \right)$$

where $\alpha_i > 0$, p_i are primes, not necessarily distinct!

<u>Applications</u>:

① $R = \mathbb{Z}$. Every f.g. abelian group M,

$$M \cong \mathbb{Z}^r \oplus \mathbb{Z}/(a_1) \oplus \dots \oplus \mathbb{Z}/(a_m),$$

$1 < a_i$, $a_1 | a_2 | \dots | a_m$, so that

$$M \cong \mathbb{Z}^r \oplus \left(\bigoplus_{i=1}^{T} \mathbb{Z}/(p_i^{\alpha_i}) \right), \ p_i - \text{primes}.$$

② $R = \mathbb{F}$, a field. Any ideal is either $\{0\}$ or $\mathbb{F}$ itself.

$\therefore$ $\forall$ $\mathbb{F}$-v.sp. is iso' to $\mathbb{F}^r$ for some unique r.

[Warning! Highly circular logic!]

③ $R = \mathbb{F}[x]$, $\mathbb{F}$ a field.

M — f.g. R-module

$\updownarrow$ $\qquad\qquad$ $\updownarrow$

(M, T) f. dim'l $\mathbb{F}$-v.sp. with linear T.

Since $\dim_{\mathbb{F}}(\mathbb{F}[x]) = \infty$, M is torsion

$$\therefore M \cong \mathbb{F}[x]/(a_1(x)) \oplus \cdots \oplus \mathbb{F}[x]/(a_m(x))$$

$\deg(a_i(x)) > 0$, $a_i(x)$ monic,

$a_1(x) \mid \cdots \mid a_m(x)$ (and are unique)

Each $\mathbb{F}[x]/(a_i(x))$ is a sub-v.sp. of M, preserved by T. A basis is given by

$\{1, x, \ldots, x^{d-1}\}$, where $d = \deg(a_i(x))$

If $a_i(x) = x^d + \ldots + c_1 x + c_0$, then T acts by

$$\begin{bmatrix} 0 & 0 & & -c_0 \\ 1 & 0 & & -c_1 \\ & 1 & \ddots & \vdots \\ & & 1 & -c_{d-1} \end{bmatrix} \longleftarrow \text{companion matrix of } a_i(x)$$

$\Rightarrow$ Char. poly. of T on this space is $a_i(x)$, the min. poly. is also $a_i(x)$, b/c

$$\cong \mathbb{F}[x]/(a_i(x))$$

That is $a(x)$ kills $\mathbb{F}[x]/a(x)$ and if $b(x)$ kills this module,

$$b(x)\cdot 1 \in (a(x)) \implies a(x) \mid b(x)$$

Since $a(x) \mid$ min. poly, $\deg(a(x)) = \dim(\mathbb{F}[x]/a(x))$

$\implies \deg(a(x)) = \deg(\text{char. poly})$.

$\therefore$ $a(x) = \text{char. poly} = \text{min. poly}$

Back to general case $(*)$,

$$\begin{cases} \text{min. poly. of } T = a_m(x) \\ \text{char. poly. of } T = a_1(x)\cdot \ldots \cdot a_r(x) \end{cases}$$

<u>Corollary</u>: $\mathbb{F}$ - field, $GL_n(\mathbb{F})$ acts on $M_n(\mathbb{F})$ by $M \mapsto gMg^{-1}$ (change of basis).

Structure theorem $\implies$ each $M \in M_n(\mathbb{F})$ is conjugate to a matrix of the form

$$\begin{bmatrix} C_1 & & & 0 \\ & C_2 & & \\ & & \ddots & \\ 0 & & & C_s \end{bmatrix}, \text{ each } C_i = \begin{bmatrix} 0 & & & 0 & * \\ 1 & 0 & & & \vdots \\ & \ddots & \ddots & & \\ & & & 0 & * \\ 0 & & & 1 & * \end{bmatrix}$$

s.t. $\sum_{i=1}^{s} \text{size}(C_i) = n$ and

$\Delta(C_1) \mid \Delta(C_2) \mid \dots \mid \Delta(C_s)$

char. poly.

Corollary: (Invariant factors)

Let $A, B \in M_n(\mathbb{F})$, $\mathbb{F} \subseteq K$ a field, then

A is conjugate to B over $\mathbb{F}$ $\Longleftrightarrow$

$\Longleftrightarrow$ A is conjugate to B over K.

Proof:

$$A \begin{array}{l} \nearrow (\mathbb{F}^n, T_A) \cong \mathbb{F}[x]/(a_i(x)) \\ \searrow (K^n, T_A) \cong K[x]/(a_i(x)) \end{array}$$

So $\{a_i(x)\}$ are also the invariant factors over K. Since conj. classes are determined by those, done.

$\square$

Structure theorem ($R=\mathbb{F}[x]$) in elementary divisors form. Same setting:

$$V \cong \bigoplus_{i=1}^{t} \mathbb{F}[x]/(f_i(x)^{a_i}) \quad , \; f_i \text{ irreducible poly}, \; a_i > 0.$$

Suppose that $\mathbb{F}$ is an algebraically closed field, i.e. any non-const. poly. is a product of linear terms (e.g. $\mathbb{C}$).

Then must have $f_i(x) = (x-\lambda_i)$, to understand V, can assume

$$V = \mathbb{F}[x]/(x-\lambda)^a \quad \text{(one block case)}$$

<u>Note</u>: Polynomials

$\mathcal{B} = \{(x-\lambda)^{a-1}, \dots, (x-\lambda), 1\}$ are a basis for V.

In this basis, $(x-\lambda)$ acts by $\begin{bmatrix} 0 & 1 & & 0 \\ & 0 & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{bmatrix}$

Thus, our linear transformation T acts by $x = (x-\lambda) + \lambda$, namely we got the JCF:

$$\begin{bmatrix} 0 & \lambda & & 0 \\ & \ddots & \ddots & \\ & & \ddots & \lambda \\ 0 & & & 0 \end{bmatrix} \quad \text{JCF of } T!$$

§ 3.d Localization

October-22-10
8:30 AM

Localization is the algebraic way to pass to a local neighbourhood, in analogy to passing to a local neighbourhood of a point on a manifold.

For this section, assume R to be a commutative non-zero ring.

<u>Def</u>: A set $S \subseteq R$ is called multiplicative if $1 \in S$ and

$$x, y \in S \implies xy \in S$$

<u>Examples</u>: * $S = R \setminus \{0\}$

* Let $I \triangleleft R$ be a prime ideal, meaning that $xy \in I \implies$ either $x \in I$ or $y \in I$ and $I \neq R$ (equivalently R/I is an integral domain). Set $S = R \setminus I$ (set minus!)

* $x \in R$, $S = \{1, x, x^2, \dots\}$

* M manifold with $p_0 \in M$; R - functions defined locally around p_0, complex-valued.

$$I = \{\text{functions vanishing at } p_0\}$$

$\mathrm{eval} : R \to \mathbb{C}$, $\mathrm{eval}(f) = f(p_0)$

This gives us an iso' $R/_I \cong \mathbb{C} \Rightarrow I$ prime

$\Rightarrow S = R \setminus I$ (functions <u>NOT</u> vanishing at p.)

—— ∘ ——

Fix R, S. Let M be an R-module. Define an equivalence relation on $M \times S$,

$$(m_1, s_1) \sim (m_2, s_2) \iff \exists t \in S : t(s_2 m_1 - s_1 m_2) = 0$$

↳ Soon the equiv. classes will be denoted $\frac{m_1}{s_1}$.

* reflexive : $(m, s) \sim (m, s)$, take $t = 1$ ✓

* symmetric : $(m_1, s_1) \sim (m_2, s_2) \Rightarrow (m_2, s_2) \sim (m_1, s_1)$ by taking the same t. ✓

* transitivity : $(m_1, s_1) \sim (m_2, s_2)$, $(m_2, s_2) \sim (m_3, s_3)$

$\Rightarrow \exists t_1, t_2$ s.t. $\begin{cases} t_1(s_2 m_1 - s_1 m_2) = 0 \\ t_2(s_3 m_2 - s_2 m_3) = 0 \end{cases}$, but

$$s_2(s_1 m_3 - s_3 m_1) = s_1(s_2 m_3 - s_3 m_2) + s_3(s_1 m_2 - s_2 m_1) \Rightarrow$$

$$\Rightarrow (t_1 t_2 s_2)(s_1 m_3 - s_3 m_1) = 0 \Rightarrow$$

$$\Rightarrow (m_1, s_1) \sim (m_3, s_3) \quad ✓$$

Denote by $\frac{m}{s}$ the equivalence class of (m,s)

$$M[S^{-1}] = \left\{ \frac{m}{s} : m \in M,\ s \in S \right\}$$

<u>Example</u> : $R[S^{-1}] = \left\{ \frac{r}{s},\ r \in R,\ s \in S \right\}$

<u>Proposition</u>: 1. $R[S^{-1}]$ is a ring and the map $\varphi : R \to R[S^{-1}],\ r \mapsto \frac{r}{1}$ is a ring homo', but not necessarily injective.

2. $M[S^{-1}]$ is an $R[S^{-1}]$-module with operations

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} := \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}$$

$$\frac{r}{s} \cdot \frac{m_1}{s_1} := \frac{r m_1}{s s_1}, \quad 0 := \frac{0}{1},\ 1 := \frac{1}{1}.$$

<u>Proof</u>: Exercise. $\square$

Thus, localization is a functor $\underline{R\mathrm{Mod}} \to \underline{R[S^{-1}]\mathrm{Mod}}$ with the action on morphisms given by

$$(f : M \to N) \xmapsto{\mathrm{loc}} (f[S^{-1}] : M[S^{-1}] \to N[S^{-1}])$$

where $(f[S^{-1}])\left(\frac{m}{s}\right) := \frac{f(m)}{s}$.

↳ This defines a covariant functor.
<u>Proof</u>: Exercise.

Def: • A sequence of R-modules and R-module homo'

$$\cdots \longrightarrow M_n \xrightarrow{f_n} M_{n+1} \longrightarrow \cdots$$

is called a complex if $f_{n+1} \circ f_n = 0 \ \forall n$.

• Equivalently, $\mathrm{im}(f_n) \subseteq \ker(f_{n+1}) \ \forall n$.

• Such a sequence is called an exact sequence if $\mathrm{im}(f_n) = \ker(f_{n+1}) \ \forall n$.

Example: * Let $f: M \twoheadrightarrow N$ be surjective, $L = \ker(f)$, then

$$0 \longrightarrow L \longrightarrow M \xrightarrow{f} N \longrightarrow 0$$

is an exact sequence.

* A short exact sequence is a sequence

$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0$$

with $\mathrm{im}(f_1) = \ker(f_2)$, f_1 injective, f_2 surjective.

Def: Let R_1, R_2 be rings. A covariant functor $F: \underline{R_1\mathrm{Mod}} \longrightarrow \underline{R_2\mathrm{Mod}}$ is called additive if $\forall M_1, M_2 \in \mathrm{Obj}(\underline{R_1\mathrm{Mod}})$, $\forall f_1, f_2 \in \mathrm{Hom}(M_1, M_2)$,

$$F(f_1 + f_2) = Ff_1 + Ff_2$$

Exercise: If F is additive, $F(0)=0$ for both the 0 module & 0 homo.

Rmk: If F is additive, and
$$0 \to M_1 \to M_2 \to M_3 \to 0$$
is an exact sequence, then
$$F(0) = 0 \to F(M_1) \to F(M_2) \to F(M_3) \to 0 = F(0)!$$
is a complex.

Proof: Exercise.

Def: If F is s.t. $0 \to M_1 \to M_2 \to M_3 \to 0$ is exact $\Longrightarrow$

$\Longrightarrow$ $0 \to F(M_1) \to F(M_2) \to F(M_3) \to 0$ is exact,

then F is said to be an exact functor.

Proposition: Localization is an exact functor

Proof: Let $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ be exact.
Localization is obviously additive, so we already know that
$$0 \to M_1[S^{-1}] \xrightarrow{f[S^{-1}]} M_2[S^{-1}] \xrightarrow{g[S^{-1}]} M_3[S^{-1}] \to 0$$
is a complex, i.e. $\operatorname{im}(f[S^{-1}]) \subseteq \ker(g[S^{-1}])$

Let us check that $\underset{\overset{\Vert}{\psi}}{\ker(g[S^{-1}])} \subseteq \underset{\overset{\Vert}{\varphi}}{\operatorname{im}(f[S^{-1}])}$,
φ injective, ψ surjective.

* $\varphi\left(\frac{m_1}{s_1}\right) = 0 \implies \frac{f(m_1)}{s_1} = \frac{0}{1}$

but then, $\exists s \in S$ s.t. $s f(m_1) = 0 \implies$
$\implies f(sm_1) = 0 \implies sm_1 = 0 \implies$
$\implies \frac{sm_1}{ss_1} = 0 \implies \frac{m_1}{s_1} = 0$

Thus φ is injective. ✓

* ψ surjective $\longrightarrow$ Exercise ✓

* Let $\frac{m_2}{s_2} \in \ker\psi$, that is $\frac{g(m_2)}{s_2} = 0 \in M_3[S^{-1}]$

$\implies \exists s \in S$ s.t. $sg(m_2) = g(sm_2) = 0$

As the first sequence was exact, $\mathrm{im}(f) = \ker(g)$
$\implies \exists m_1 \in M_1$ s.t. $f(m_1) = sm_2$.

Then $\varphi\left(\frac{m_1}{ss_2}\right) = \frac{sm_2}{ss_2} = \frac{m_2}{s_2}$

$\therefore \ker\psi \subseteq \mathrm{im}\,\varphi$.

$\square$

Behaviour of ideals under localization

October-27-10
11:18 AM

R is a commutative ring,
S is a multiplicative set.

Let $I \lhd R$, then $I[S^{-1}] \lhd R[S^{-1}]$.
Indeed, $0 \to I \hookrightarrow R \twoheadrightarrow R/I \to 0$ exact
$\Longrightarrow$ $0 \to I[S^{-1}] \hookrightarrow R[S^{-1}] \twoheadrightarrow (R/I)[S^{-1}] \to 0$
is also exact.

$\therefore$ $I[S^{-1}] \subseteq R[S^{-1}]$, and $I[S^{-1}]$ is an $R[S^{-1}]$-module $\Rightarrow$ $I[S^{-1}]$ is an ideal.

$I[S^{-1}] = \left\{ \frac{i}{s} : i \in I, s \in S \right\}$ is the ideal generated by $\varphi(I)$ in $R[S^{-1}]$, where

$$\varphi : R \longrightarrow R[S^{-1}], \quad r \longmapsto \frac{r}{1}$$

$$\therefore \quad I[S^{-1}] = \langle \varphi(I) \rangle_{R[S^{-1}]}$$

Conversely, $\forall \varphi : R \to R[S^{-1}]$ ring homo',
if $J \lhd R[S^{-1}]$, $\varphi^{-1}(J) \lhd R$.

We will now investigate to what extent does the "unlocalization" map φ^{-1} actually undo the effects of localizing a ring R.

Recall:

R = comm. ring, $S \subseteq R$ mult. set ($1 \in S$, $x, y \in S \Rightarrow xy \in S$)

M = R-module

$M[S^{-1}] = \left\{ \frac{m}{s} : m \in M, s \in S \right\}$ ← an $R[S^{-1}]$-module.

$R[S^{-1}] = \left\{ \frac{r}{s} : r \in R, s \in S \right\}$ is a ring

Here $\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{m_1 s_2 + s_1 m_2}{s_1 s_2}$, etc.

$\varphi : R \to R[S^{-1}]$, $\varphi(r) = \frac{r}{1}$
not necessarily injective!

If $I \lhd R$, then $\underbrace{\langle \varphi(I) \rangle}_{\text{ideal generated in } R[S^{-1}]} = I[S^{-1}]$

($I \subseteq R \Rightarrow I[S^{-1}] \subseteq R[S^{-1}]$ b/c loc. is exact)

If $J \lhd R[S^{-1}]$, then $\varphi^{-1}(J) = \left\{ j \in R : \frac{j}{1} \in J \right\}$ is an ideal of R.

Claim: $\varphi^{-1}(J)[S^{-1}] = J$

Proof: If $\varphi : A \to B$ a homo of rings, $J \lhd B \Rightarrow \langle \varphi(\varphi^{-1}(J)) \rangle_B \subseteq \langle J \rangle_B = J$

$\therefore$ $[\subseteq]$ is clear.

For $[\supseteq]$, let $\frac{j}{s} \in J \Rightarrow \frac{s}{1} \cdot \frac{j}{s} = \frac{j}{1} \in J$ b/c ideal

$\Rightarrow j \in \varphi^{-1}(J)$ and so

$$\frac{j}{s} \in \varphi^{-1}(J)[s^{-1}] \quad \checkmark$$

$\square$

<u>Claim</u>: $I \lhd R$, prime ideal, $I \cap S = \emptyset$.

Then $\varphi^{-1}(I[s^{-1}]) = I$.

<u>Proof</u>: $[\supseteq]$ is clear by part $[\subseteq]$ of previous claim.

$[\subseteq]$ Let $x \in \varphi^{-1}(I[s^{-1}]) \Rightarrow \frac{x}{1} \in I[s^{-1}]$

$\Rightarrow \frac{x}{1} = \frac{i}{s}$ for some $i \in I$, $s \in S$.

b/c we know $\langle \varphi(I) \rangle = I[s^{-1}]$?

$\Rightarrow \exists t \in S : t(sx - i) = 0 \Rightarrow$

$\Rightarrow \exists t \in S : (ts)x = ti \in I$.

I prime $\Rightarrow ((ts)x \in I \Rightarrow$ either $ts \in I$ or $x \in I)$

As $I \cap S = \emptyset$, $ts \notin I$ (b/c $t, s \in S \Rightarrow ts \in S$)

$\therefore x \in I$

$\square$

Corollary: Let I_0 be the prime ideal of R, let $S = R \setminus I_0$. Then $\exists$ bijection

$$\{\text{prime ideals } I \subseteq I_0\} \xleftrightarrow{\varphi} \{\text{ideals of } R[S^{-1}]\}$$

$$\varphi(I) = I[S^{-1}]$$

Proof: Apply both claims.

$\square$

In particular, $R[S^{-1}]$ (in this case) is a local ring, i.e. has a unique maximal ideal, which is $I_0[S^{-1}]$.

Local properties of modules and rings

October-25-10
9:55 AM

Def: We call a property α of modules, resp. rings, *local* if

$$M \text{ has } \alpha \iff M[S^{-1}] \text{ has } \alpha$$

where $S = R \setminus \mathfrak{p}$ $\forall$ prime ideal $\mathfrak{p}$, and M is an R-module or $M=R$ is a ring.

Example: Being 0 is a local property.

* If $M = \{0\}$, then $M[S^{-1}] = \{0\}$, $\forall S$.
* If $M \ni m \neq 0$, $\operatorname{Ann}(m) = \{r \in R : rm = 0\} \neq R$. Let $\mathfrak{p}$ be a maximal ideal containing $\operatorname{Ann}(m)$, and $S = R \setminus \mathfrak{p}$.

Claim: $\frac{m}{1} \in M[S^{-1}]$ is not zero.

If $\frac{m}{1} = \frac{0}{1}$, $\exists t \in S$, $tm = 0 \Rightarrow$
$\Rightarrow t \in \operatorname{Ann}(m) \subseteq \mathfrak{p}$ Contradiction!

Notation: If $\mathfrak{p}$ is a prime ideal,

$$M_{\mathfrak{p}} := M[S^{-1}], \quad S = R \setminus \mathfrak{p}.$$

Proposition: A complex of R-modules

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

is exact iff

$$0 \longrightarrow M_{1\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} M_{2\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} M_{3\mathfrak{p}} \longrightarrow 0$$

is exact $\forall$ prime ideals $\mathfrak{p}$.

Proof (sketch):

* $\ker(f_{\mathfrak{p}}) = [\ker(f)]_{\mathfrak{p}}$
  (using that localization is an exact functor)
  $\operatorname{Im}(f_{\mathfrak{p}}) = [\operatorname{Im}(f)]_{\mathfrak{p}}$

* Use the previous example and the above relations.

$\square$

Remark: α = "Free" is NOT a local property of R-modules.

Let R be an ID, then $\forall$ prime $\mathfrak{p}$,

$$\varphi : R \longrightarrow R_{\mathfrak{p}} \quad (R[S^{-1}],\ S = R \setminus \mathfrak{p})$$

is injective.

So, we shall view $R \subseteq R_{\mathfrak{p}}$ (as a subring in fact).

Fraction field

October-25-10
10:15 AM

$R = ID.$

Let $S = R \setminus \{0\}$, then

$$R \subseteq R[S^{-1}] = \left\{ \frac{r}{s} : r, s \in R,\ s \neq 0 \right\}$$

$$=: \mathrm{Frac}(R)$$

the fraction field of R

$R[S^{-1}]$ <u>is</u> a field, as $0 = \frac{r}{s} \in R[S^{-1}]$,

$r \neq 0$, $\Longrightarrow \frac{s}{r} \cdot \frac{r}{s} = 1$. ✓

We view $R \subseteq R_p \subseteq \mathrm{Frac}(R)$

$r \longmapsto \frac{r}{1}$, $\frac{r}{s} \longmapsto \frac{r}{s}$

N.B. $\mathrm{Frac}(R)$ is the minimal field containing R.

Proposition: Let $I \triangleleft R$ an ideal. Then

$$I = \bigcap_{\substack{\mathfrak{p} \triangleleft R \\ \text{prime}}} I_{\mathfrak{p}}$$

N.B. The intersection is viewed in $\mathrm{Frac}(R)$!

Proof: $[\subseteq]$ is clear.

$[\supseteq]$ Let $J = \bigcap_{\mathfrak{p} \triangleleft R} I_{\mathfrak{p}}$, let $j \in J$ and

$K = \{ r \in R : rj \in I \}$ is an ideal of R.

If $K \neq R$, $K \subseteq$ max'l ideal $\mathfrak{p}$ $\Longrightarrow$

$\Longrightarrow j \in I_{\mathfrak{p}}$, but $j = \frac{i}{s}$, $i \in I$, $s \in S = R \setminus \mathfrak{p}$

$\Longrightarrow sj \in I \Longrightarrow s \in K \subseteq \mathfrak{p}$ Contradiction ⋇

$\therefore K = R \Longrightarrow 1 \in K \Longrightarrow j \in I$

□

§ 3.e Injective and projective limits

October-27-10
9:33 AM

→ This generalizes the notions of co-product & product resp.

Let I be a poset. We can view I as a category $\underline{I}$ with $\mathrm{Obj}(\underline{I}) = \{i \in I\}$,

$$\mathrm{Hom}(x,y) = \begin{cases} i_{xy} & \text{if } x \le y \\ \emptyset & \text{else} \end{cases}$$

formal symbol

$$x \le y \le z \implies i_{yz} \circ i_{xy} = i_{xz}.$$

<u>Def</u>: Let $\underline{C}$ be a category. An injective (direct) system indexed by I is a covariant functor $\underline{I} \longrightarrow \underline{C}$

A projective (inverse) system is a contravariant functor $\underline{I} \longrightarrow \underline{C}$.

Equivalently, an injective system:

$\forall i \in I$, given $C_i \in \mathrm{Obj}(\underline{C})$,
$\forall x \in I$, $f_{xx} : C_x \longrightarrow C_x$ identity,
$\forall x \le y$, $f_{xy} : C_x \longrightarrow C_y$ s.t.

$$x \le y \le z \implies f_{yz} \circ f_{xy} = f_{xz}$$

$$\begin{tikzcd} C_x \arrow[r] \arrow[dr] & C_y \arrow[d] \arrow[dl, phantom, "\circlearrowright"] \\ & C_z \end{tikzcd}$$

$\Big\}$ $f_{xy} : C_y \longrightarrow C_x$ in the case of projective systems.

Examples

- I = any set with <u>no</u> $x, y \in I$, s.t. $x \le y$
- $I = \mathbb{Z}_{>0}$, $n \le m$ if $n | m$
  $\underline{C}$ = abelian groups.

set $C_n = \frac{1}{n}\mathbb{Z} \xhookrightarrow{i_{nm}} \frac{1}{m}\mathbb{Z} = C_m$, if $n|m$.

Then $(\{C_n\}, \{i_{nm}\})$ is a direct system in $\underline{C}$.

- For the same I, set

$$C_n = \mathbb{Z}/n\mathbb{Z} \xleftarrow[p_{nm}]{} \mathbb{Z}/m\mathbb{Z} = C_m$$

$$x \bmod n \longleftarrow\!\shortmid\; x \bmod m \quad \text{if } n|m$$

Then $(\{C_n\}, \{p_{nm}\})$ is an inverse system.

- $I = \mathbb{Z}_{>0}$, $n \le m$ if $n \le m$ (usual order)
  Fix a prime p.

$$C_n = \mathbb{Z}/p^n\mathbb{Z} \longleftarrow \mathbb{Z}/p^m\mathbb{Z} = C_m$$

defines an inverse system, similar to the above one.

- More generally, if R is a commutative ring, $I \triangleleft R$,

$$C_n = R/I^n$$

For $n \leq m$,

$$\begin{array}{ccc} C_n & \longleftarrow & C_m \\ x \bmod I^n & \longmapsfrom & x \bmod I^m \end{array}$$

This is an inverse system in the category $\underline{C}$ of commutative rings.

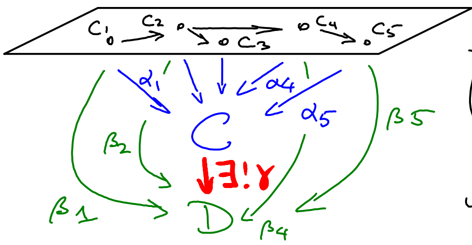
<u>Def</u>: Let $(\{C_i\}, \{f_{ij}\}_{i\leq j})$ be direct system in $\underline{C}$. Its direct (injective) limit,

$$\varinjlim_{i\in I} C_i$$

is an object C in $\underline{C}$ with morphisms $\alpha_i : C_i \to C$, such that $\forall i \leq j$, $\alpha_j \circ f_{ij} = \alpha_i$, and with the universal property:

Given any $D \in \mathrm{Obj}(\underline{C})$ with morphisms $\beta_i : C_i \to D$, s.t. $\forall i \leq j$ $\beta_j \circ f_{ij} = \beta_i$, $\exists !\, \gamma : C \to D$ s.t.

$$\gamma \circ \alpha_j = \beta_j \quad \forall j \in I.$$



Everything must commute here!

Def: Let $(\{C_i\}, \{f_{ij}\}_{i\le j})$ be an inverse system in $\underline{C}$. The inverse (projective) limit,

$$\varprojlim C_i$$

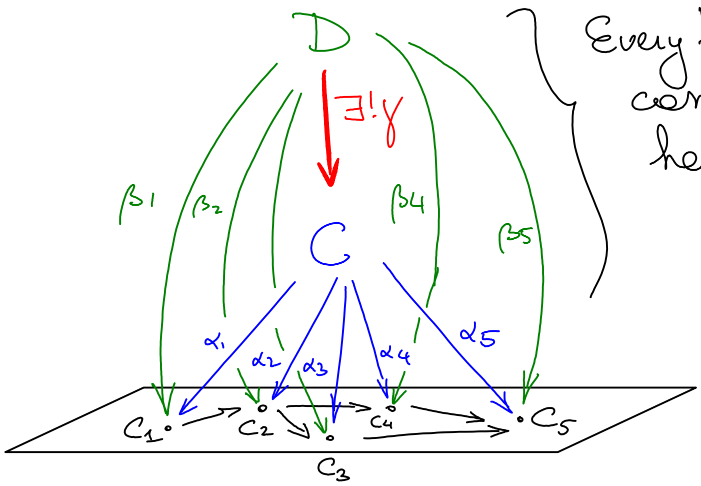
is an object C of $\underline{C}$ with morphisms

$$p_i : C \longrightarrow C_i, \text{ s.t. } \forall i\le j \; f_{ij}\circ p_j = p_i$$

and the universal property: given any $D \in Obj(\underline{C})$ with morphisms

$$q_i : D \longrightarrow C_i, \text{ s.t. } \forall i \le j \; f_{ij}\circ q_j = q_i$$

$$\exists!\, \gamma : D \to C \text{ s.t. } \forall i,\; p_i\circ\gamma = q_i$$



Everything commutes here

Example : R - any ring
I - discrete poset (no order)

$\underline{C} = \underline{R\mathrm{Mod}}$. We proved that

$$\varinjlim M_i = \bigoplus_{i \in I} M_i \quad \text{(coproduct)}$$

$$\varprojlim M_i = \prod_{i \in I} M_i \quad \text{(product)}$$

Theorem : Let R be a ring. Direct and inverse limits exist in $\underline{R\mathrm{Mod}}$.

Proof: Let $(\{M_i\}, \{f_{ij}\})$ be a direct system.

We construct $\varinjlim M_i$ as a quotien module of $\bigoplus_{i \in I} M_i$. Let

$\lambda_i : M_i \hookrightarrow \bigoplus_{i + I} M_i$ be the canonical inclusion.

Let $W \subseteq \bigoplus M_i$ be the submodule generated by the elements $\{\lambda_i(a) - \lambda_j(f_{ij}(a)) \mid i \leq j, a \in M_i\}$
Let $C = \bigoplus M_i / W$ with

$\alpha_i : M_i \to C$, the composition $M_i \xrightarrow{\lambda_i} \bigoplus M_i \to C$
$a \longmapsto \lambda_i(a) + W$

Need to check: $\alpha_j \circ f_{ij} = \alpha_i$

Let $a \in M_i$, $\alpha_i(a) = \lambda_i(a) + W$, and
$\alpha_j(f_{ij}(a)) = \lambda_j(f_{ij}(a)) + W \Rightarrow$ OK by construction.

Suppose now that $D \in \underline{\text{RMod}}$ is given, with

$\beta_i : M_i \to D$, $\beta_j \circ f_{ij} = \beta_i$ $\forall i \leq j$.

The map $\pi : \bigoplus M_i \to C$, $x \mapsto x + W$ satisfies $\alpha_i = \pi \circ \lambda_i$ by def. of α_i's.

As $\bigoplus_i M_i = \coprod_i M_i$, $\exists ! \ \delta : \bigoplus_i M_i \to D$ s.t. $\delta \circ \lambda_i = \beta_i$.

Now $\delta (\lambda_i(a) - \lambda_j(f_{ij}(a))) =$
$= \beta_i(a) - \beta_j(f_{ij}(a)) = \beta_i(a) - \beta_i(a) = 0$

$\therefore \delta$ induces a map $\gamma : C \to D$ s.t. $\gamma \circ \alpha_i = \beta_i$ by 1st iso theorem.

Furthermore, if $\gamma' : C \to D$ is another such map, $\gamma' \equiv \gamma$ on all elements of the form

$$\{ \alpha_i(a) : i \in I, a \in M_i \}$$

But these elements generate $C \Rightarrow \gamma \equiv \gamma'$ on the whole of C.

$\therefore$ Injective limits exist. ✓

Suppose $(\{M_i\}, \{f_{ij}\})$ an inverse system in $\underline{\text{RMod}}$, ($\forall i \leq j$, $f_{ij} : M_j \to M_i$)

Let $C \subseteq \prod_{i=I} M_i$ be

$$\{(m_i)_i : f_{ij}(m_j) = m_i \ , \forall i \le j\}$$

Then C is an R-submodule of $\prod_{i\in I} M_i$.

The maps $p_i : C \to M_i$ are simply the projection maps $\prod M_i \to M_i$ restricted to C.

$$f_{ij}(p_j(\{m_\ell\})) = f_{ij}(m_j) = m_i = p_i(\{m_\ell\})$$

Suppose, we are given D, $q_i : D \to M_i$, $f_{ij} \circ q_j = q_i$

We know that $\exists ! \gamma : D \to \prod_{i\in I} M_i$ s.t.

unrestricted projection $\longrightarrow$ $p_i \circ \gamma = q_i$

We only need to check that $\mathrm{im}(\gamma) \subseteq C$, namely that $\forall d \in D$,

$$[\gamma(d)]_i = q_i(d) \stackrel{!}{=} f_{ij}(q_j(d)) = f_{ij}([\gamma(d)]_j)$$

$\square$

Remark: The uniqueness of both limits follows from the usual arguments using the universal property.

Examples

* The pull-back (or fiber product) is the inverse limit of

$$\begin{tikzcd} & B \arrow[d, "\beta"] \\ A \arrow[r, "\alpha"] & C \end{tikzcd}$$

In this case, it is denoted by $A \times_C B$:

$$\begin{tikzcd} & A \times_C B \arrow[dl] \arrow[dr] & \\ A \arrow[dr, "\alpha"'] & & B \arrow[dl, "\beta"] \\ & C & \end{tikzcd}$$

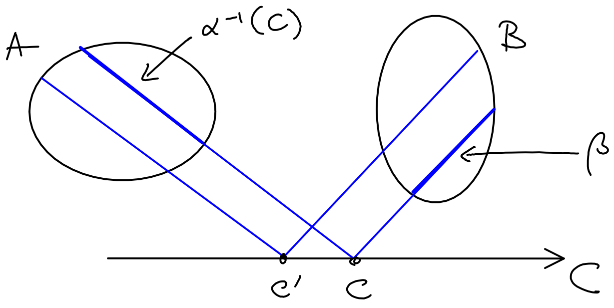
N.B. The map to C is implicitly given by the composition of $A \times_C B \to A \to C$ (say).

What is $A \times_C B$?

$$A \times_C B = \varprojlim \{(a,b,c) : a \in A, b \in B, c \in C, C = \alpha(A) = \beta(B)\}$$

$$= \varprojlim \{(a,b) : a \in A, b \in B, \alpha(A) = \beta(B)\}$$

$$\overset{\text{Sets}}{=} \coprod_{c \in C} \alpha^{-1}(c) \times \beta^{-1}(c)$$



* The push-out is the direct limit of

$$A \xleftarrow{\alpha} C \xrightarrow{\beta} B$$

One finds, by construction, that the push-out M is

$$M \cong A \oplus B \,/\, \{(\alpha(c), -\beta(c)) : c \in C\}$$

* The I-adic completion: R - ring, $I \triangleleft R$ two sided ideal of R.
The inverse system of R-modules:

$$\cdots \longrightarrow R/I^n \longrightarrow R/I^{n-1} \longrightarrow \cdots \longrightarrow R/I .$$

$\therefore$ $\hat{R} = \varprojlim_n R/I^n$ exists, and

$$\hat{R} = \{(\ldots, r_n, r_{n-1}, \ldots, r_1) \mid r_n \in R/I^n,\ r_{n+1} \equiv r_n \bmod I^n\}$$

↳ $\hat{R}$ is a ring, $(r_n)_n \cdot (s_n)_n = (r_n s_n)_n$, and the map $R \longrightarrow \hat{R}$, $r \mapsto (\ldots r, r, \ldots, r)$ is a ring homo with kernel $\bigcap_{n \geq 1} I^n$, which may be non-trivial.

For example, take $R = \mathbb{C}[t^{1/n} : n \in \mathbb{N}]$, and $I = (\{t^{1/n} : n \geq 1\}) = I^m \ \forall m \in \mathbb{N}$, $R/I \cong \mathbb{C}$ and the kernel is large.

However in many important cases $R \hookrightarrow \hat{R}$ injects
for every $I \triangleleft R$, $I \neq R$.

↳ see Krull's theorem

<u>Rmk</u>: The completions serve to perform infinitesimal analysis of R.

Take $R = k[t]$, where k is any commutative ring, $I = (t)$. Then the I-adic completion $\hat{R}$,

<u>Exercise</u>: $\hat{R} = \varprojlim k[t]/(t^n) \overset{!}{\cong} k[\![t]\!]$

$$k[\![t]\!] \ni f(t) \longmapsto (\dots, f(t) \bmod t^2, f(t) \bmod t) \in \hat{R}$$

In particular, $f(t) = \sum a_i t^i \longmapsto (\dots, a_1 t + a_0, a_0)$, so we get from a poly. ring to a power series ring!

* $R = \mathbb{Z}$, $I = (p)$ for some prime p.

$$\dots \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

$$\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \left\{ (\dots, r_n, \dots, r_1) \,\middle|\, \begin{array}{l} r_n \in \mathbb{Z}/p^n\mathbb{Z} \\ r_{n+1} = r_n \bmod p^n \end{array} \right\}$$

↳ Commutative ring.

<u>Rmks</u>: • $\mathbb{Z}_p$ is a compact Hausdorff space with the discrete topology:

b/c by Tychonoff, $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$ is compact and Hausdorff as each $\mathbb{Z}/p\mathbb{Z}$ is finite. $\mathbb{Z}_p$ is a closed subset of $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z} \implies$
$\implies$ it is itself compact & Hausdorff.

• $\mathbb{Z}_p$ is an integral domain:

divides exactly

Suppose $(r_i)_i \cdot (s_i)_i = (0)_i$ but $\exists n : r_n \neq 0$.
$\implies \exists\ 0 \leq j < n$ s.t. $p^j \| r_n$. To show $(s_i) = (0)$ it is enough to show that $\forall m$, $p^m \| s_i$ for i large
$\left(\implies p^m | s_i\ \forall i \implies (s_i) = (\ldots, *, \overset{m^{th}}{0}, \ldots, 0) \implies (s_i) = (0)\right)$

We know: $p^{n+\alpha} \mid r_{n+\alpha} s_{n+\alpha}$ $\forall \alpha \geq 0$.
Since $p^j \| r_n \implies p^j \| r_{n+\alpha}$ $\forall \alpha \geq 0$,

$$p^{n+\alpha-j} \mid s_{n+\alpha} \quad \forall \alpha \geq 0$$

$\therefore \forall \alpha \geq m+j-n$, $p^m \| s_{n+\alpha}$ ✓ <u>done</u>!

Define a function $v : \mathbb{Z}_p \to \mathbb{Z}$ (valuation)

$$v(r) = v((\ldots, r_n, \ldots, r_1)) = \max\{n : r_n = 0\} = \max\{n : p^n | r\}$$

<u>Exercise</u>: ν is a discrete valuation, that is
1. $\nu(x) \geq 0$ and finite $\forall x \neq 0$.
2. $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$ with equality when $\nu(x) \neq \nu(y)$
3. $\nu(xy) = \nu(x) + \nu(y)$

Further, under $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$, $z \mapsto (\dots, z, \dots, z)$, if $z = p^\alpha \cdot m$, $(m,p) = 1$, then $\nu(z) = \alpha$.

<u>Claim</u>: The function $d: \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{R}_+$

$$d(x,y) = p^{-\nu(x-y)}$$

is a <u>metric</u> on $\mathbb{Z}_p$.

- $d(x,y) \geq 0$ and $= 0$ iff $x = y$ ($\Longleftrightarrow$ (1) in the exercise)
- $d(x,y) = d(y,x) \Longleftrightarrow \nu(z) = \nu(-z)$ ✓
- $d(x,z) \leq d(x,y) + d(y,z)$, in fact the strong triangle inequality holds
  $$d(x,z) \leq \max\{d(x,y), d(y,z)\}$$
  with equality if $d(x,y) \neq d(y,z)$ (follows from (2))
  ↳ Any triangle is isoceles.

The topology induced on $\mathbb{Z}_p$ by $d(\cdot,\cdot)$ agrees with the topology we already have (as a subspace of $\prod_n \mathbb{Z}/p^n\mathbb{Z}$)

ball of radius p^{-n} around 0

↳ Neighbourhoods of 0 : $\{x : \nu(x) \geq n\} =$
$= \{(r_k)_k : r_n = r_{n-1} = \dots = r_1 = 0\} =$
$= \mathbb{Z}_p \cap \left(\prod_{j \geq 1} \mathbb{Z}/p^{n+j}\mathbb{Z} \times \{0\} \times \dots \times \{0\}\right)$

These form an open local basis around 0.

Since $\mathbb{Z}_p$ is complete, it is a complete metric space. In fact, $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ w.r.t. $d(\cdot,\cdot)$.

We only need to show that $\mathbb{Z}$ is dense in $(\mathbb{Z}_p, d)$. Given m and $(\dots, r_n, \dots, r_1) \in \mathbb{Z}_p$ choose $z \in \mathbb{Z}$, $z \equiv r_m \bmod p^m$

$$v\big((z_k)-(r_k)\big) = v\big((\dots, *, \overset{m^{th}}{\overset{\downarrow}{0}}, \dots, 0)\big) \geq m$$

$$\therefore\ d(z, (r_k)_k) \leq p^{-m}.$$

<u>Exercise</u>: Let $x, y \in \mathbb{Z}_p$, then

$$x \mid y \text{ in } \mathbb{Z}_p \iff v(x) \leq v(y)$$

Deduce that if $I \lhd \mathbb{Z}_p$ is an ideal, then $I = (p^n)$ for some $n \geq 0$. So, $\mathbb{Z}_p$ has a unique prime ideal (p).

Deduce also that $\mathbb{Z}_p^\times = \{x \mid v(x) = 0\}$

<u>Rmk</u>: $(p^n) = \{(\dots *, \overbrace{0, \dots, 0}^{n})\}$,

$$\mathbb{Z}_p/(p^n) \cong \mathbb{Z}/p^n\mathbb{Z} \text{ via } (r_k)_k \longmapsto r_n$$

Lemma: (Hensel's lemma)

Let $f(x) \in \mathbb{Z}_p[x]$ be a non-zero poly. and let $\alpha_1 \in \mathbb{Z}/p\mathbb{Z}$ be such that

$$\left.\begin{array}{ll} ① & f(\alpha_1) = 0 \\ ② & f'(\alpha_1) \neq 0 \end{array}\right\} \text{ in } \mathbb{Z}/p\mathbb{Z}$$

Then $\exists \alpha \in \mathbb{Z}_p$ s.t. $f(\alpha) = 0$ and $\alpha \equiv \alpha_1 \bmod p$.

Example: Take $f(x) = x^{p-1} - 1$

This polynomial has $(p-1)$ solutions mod p by Fermat's little theorem, and they are $\{1, 2, \dots, p-1\}$.

Also, $f'(x) = (p-1)x^{p-2} \neq 0 \quad \forall x = 1, 2, \dots, p-1$

[Hensel] $\Longrightarrow \exists\ (p-1)$ distinct $(p-1)^{st}$ roots of unity in $\mathbb{Z}_p$. ✓

Proof: Suppose that given $n \geq 1$, $\forall m \leq n$, $\exists\, \alpha_m$ in $\mathbb{Z}/p^m\mathbb{Z}$ s.t. $f(\alpha_m) = 0$ in $\mathbb{Z}/p^m\mathbb{Z}$, $\alpha_m \equiv \alpha_{m-1} \bmod p^{m-1}$.

Then we will construct α_{n+1} s.t. the same holds. Thus, taking $\alpha = (\dots, \alpha_{n+1}, \alpha_n, \dots, \alpha_1)$ yields a solution of f in $\mathbb{Z}_p$, $\equiv \alpha_1 \bmod p$.

In fact, it is enough to find α_{n+1} s.t.

$f(\alpha_{n+1}) = 0$ and $\alpha_{n+1} \equiv \alpha_n \bmod p^n$

$\longrightarrow$ Pick any $\beta \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ s.t. $\beta \equiv \alpha_n \bmod p^n$

β is unique up to $\beta \rightsquigarrow \beta + \gamma$, $\gamma \in p^n\mathbb{Z}/p^{n+1}\mathbb{Z}$.

The binomial formula,

$$(x+y)^n = x^n + \binom{n}{1} x^{n-1} y + y^2 \cdot (\dots)$$

$$f(x+y) = f(x) + f'(x) y + y^2 \cdot (\dots), \ \forall \text{poly. } f.$$

$$\Rightarrow f(\beta+\gamma) = \left(f(\beta) + f'(\beta)\gamma\right) \bmod p^{n+1} \quad \text{as}$$

$$\gamma^2 \in (p^{2n}) \subseteq (p^{n+1})$$

$\Rightarrow$ To solve $f(\beta+\gamma) = 0 \bmod p^{n+1}$ is the as to solve

$$\frac{f(\beta)}{p^n} + f'(\beta)\frac{\gamma}{p^n} = 0 \bmod p$$

But $f'(\beta) \equiv f'(\alpha_1) \neq 0 \bmod p$, so we can find $\gamma/p^n \bmod p \Rightarrow$ we can find γ.

$\square$

Direct limits over a directed set

November-01-10
9:33 AM

Def: If I is a poset, we say that it is directed if $\forall i,j \in I$, $\exists k \in I$ s.t. $i \le k$ & $j \le k$.

In this case, direct limits over I have a convenient description.

Suppose $(\{M_i\}, \{f_{ij}\})$ is a direct system over a directed set I. Put an equiv. relation on $\biguplus_{i \in I} M_i$ (disjoint union of sets!): say that

$$M_i \ni m_i \sim m_j \in M_j \quad \text{if } \exists k \ge i,j \text{ s.t.}$$

$$f_{ik}(m_i) = f_{jk}(m_j)$$

And we write $[m_i]$ for the equiv. class.

Typical example: X manifold, $x_0 \in X$. For open set $U \ni x_0$, let

$$M(U) = \{\text{continuous } f : U \to \mathbb{C}\}$$

Then $U \supseteq V \Rightarrow \text{restriction}_{UV} : M(U) \to M(V)$.
$I = \{U \text{ open} : x_0 \in U\}$, I is directed b/c

both $U, V \subseteq U \cap V$

$\varinjlim \mathcal{M}(U)$ is called the group of germs of continuous functions at x_0.

$$\boxed{\begin{array}{l} f \in \mathcal{M}(U) \text{ is considered equal to} \\ g \in \mathcal{M}(V) \text{ if } \exists\, W \text{ open, } W \subseteq U \cap V \\ x_0 \in W \text{ and } f = g \text{ on } W \end{array}}.$$

Define $[m_i] + [m_j] = [f_{ik}(m_i) + f_{jk}(m_j)]$, $k \geq i,j$

$r[m_i] = [r m_i]$

↪ Call the resulting R-module M. (check that it is well-defined).

Natural maps $\mathcal{M}_i \to M$, $m_i \longmapsto [m_i]$.

<u>Proposition</u>: $\varinjlim \mathcal{M}_i \cong M$.

<u>Proof</u>: $\exists!$ map $\varinjlim \mathcal{M}_i \longrightarrow M$ (b/c

$$\begin{tikzcd} \mathcal{M}_i \arrow[rr, "f_{ij}"] \arrow[dr, "\alpha_i"] \arrow[ddr, bend right] & & \mathcal{M}_j \arrow[dl, "\alpha_j"'] \arrow[ddl, bend left] \\ & \varinjlim \mathcal{M}_i \arrow[d, dashed] & \\ & M & \end{tikzcd}$$

$[m_j] = [f_{ij}(m_i)]$ by def'n if $i \leq j = k$.)

Recall $\varinjlim \mathcal{M}_i \cong \oplus \mathcal{M}_i / W$, so this map is determined by

$$(\ldots, 0, m_i, 0, \ldots, 0) + W \longmapsto [m_i]$$

We construct the inverse map:

$$[m_i] \longmapsto (\ldots, 0, m_i, 0, \ldots, 0) + W$$

* Well-defined: enough that if $i \leq k$ & $m_k = f_{ik}(m_i)$, then have

$$\begin{array}{ccc}
[m_i] & \longmapsto & (\dots, 0, \overset{i\text{th}}{m_i}, 0, \dots) + W \\
\| & & \|? \\
[m_k] & \longmapsto & (\dots, 0, \underset{}{\overset{k\text{th}}{m_k}}, 0, \dots) + W
\end{array}$$

As $\alpha_k(f_{ik}(m_i)) - \alpha_i(m_i) \in W$, this is true.

* Not hard to verify that this is an R-module homo.

* Almost immediate that this is the inverse map.

$\square$

Examples: • $\varinjlim_n \frac{1}{n}\mathbb{Z}$.

For $n|m \Rightarrow m = nj$, $\frac{1}{n}\mathbb{Z} \longrightarrow \frac{1}{m}\mathbb{Z}$ is just

$$\frac{j}{m}\mathbb{Z} \subseteq \frac{1}{m}\mathbb{Z}$$

$\therefore \varinjlim_n \frac{1}{n}\mathbb{Z} \cong \mathbb{Q}$ and the funky order relation is just the usual identification of fractions with different denominators.

Limits and functors

November-01-10
9:03 AM

<u>Proposition</u>: Let (F,G) be an adjoint pair of covariant functors $F:\underline{C}\to\underline{D}$, $G:\underline{D}\to\underline{C}$

Then F commutes with direct limits and G commutes with inverse limits.

<u>Proof</u>: Let $(\{C_i\},\{f_{ij}\})$ be a direct system in $\underline{C}$, having the direct limit $(C,\{\alpha_i\})$.

$$\begin{tikzcd} C_i \arrow[rr, "f_{ij}"] \arrow[dr, "\alpha_i"'] & & C_j \arrow[dl, "\alpha_j"] \\ & C & \end{tikzcd} \quad \overset{F}{\rightsquigarrow} \quad \begin{tikzcd} F(C_i) \arrow[rr, "F(f_{ij})"] \arrow[dr, "F(\alpha_i)"'] & & F(C_j) \arrow[dl, "F(\alpha_j)"] \\ & F(C) & \end{tikzcd}$$

As F is a functor, $(\{F(C_i)\},\{F(f_{ij})\})$ <u>is</u> a direct system in D, b/c $F(\alpha_j)\circ F(f_{ij}) = F(\alpha_i)$ ✓

<u>Claim</u>: $(F(C),\{F(\alpha_i)\}) = \varinjlim F(C_i)$

Let $D\in \mathrm{Obj}(D)$ with morphisms $\beta_i: F(C_i)\to D$ s.t. $\beta_j\circ F(f_{ij}) = F(\beta_i)$

We have (b/c adjoint pair)

$$\mathrm{Hom}(C_i, G(D)) \cong \mathrm{Hom}(F(C_i), D)$$

$\Rightarrow$ Form $\beta_i' : C_i \to D$ using the iso above.

$$\begin{array}{ccccc}
\beta_i' \in \mathrm{Hom}(C_i, G(D)) & \cong & \mathrm{Hom}(F(C_i), D) \ni \beta_i \\
\uparrow f_{ij} & \circlearrowleft & \uparrow F(f_{ij}) \\
\beta_j' \in \mathrm{Hom}(C_j, G(D)) & \cong & \mathrm{Hom}(F(C_j), D) \ni \beta_j
\end{array}$$

$$\Longrightarrow \beta_i' = \beta_j' \circ f_{ij}$$

Using $\varinjlim C_i = C$ in $\underline{C}$, $\exists!\, \gamma' : C \to G(D)$ s.t. $\gamma' \circ \alpha_i = \beta_i'$ (by univ. prop.)

$$(*)\quad \begin{array}{ccccc}
\gamma' \in \mathrm{Hom}(C, G(D)) & \cong & \mathrm{Hom}(F(C), D) \ni \gamma \\
\downarrow \alpha_i & \circlearrowleft & \downarrow F(\alpha_i) \\
\beta_i' \in \mathrm{Hom}(C_i, G(D)) & \cong & \mathrm{Hom}(F(C_i), D) \ni \beta_i
\end{array}$$

$\therefore\ \gamma' \circ \alpha_i = \beta_i' \Longrightarrow \gamma \circ F(\alpha_i) = \beta_i$ ✓

Remains to show that γ is unique with this property. So, suppose $\tilde{\gamma} : F(C) \longrightarrow D$ be s.t. $\tilde{\gamma} \circ F(\alpha_i) = \beta_i$ $\forall i \in I$.

Using diagram $(*)$, we have $\tilde{\gamma}' : C \to G(D)$, $\tilde{\gamma}' \circ \alpha_i = \beta_i'$

But $\tilde{\gamma}' = \gamma'$ (by univ. prop.) $\Longrightarrow \tilde{\gamma} = \gamma$

↳ The case of inverse limits is symmetric.

$\square$

<u>Application</u> : Any two direct limits commute.

<u>Def</u>: If $(\{C_i\}, \{f_{ij}\})$, $(\{D_i\}, \{g_{ij}\})$ are direct systems over I, then we can define a <u>morphism</u> between them by

$$\begin{tikzcd} C_i \arrow[r, "f_{ij}"] \arrow[d, "h_i"'] \arrow[dr, phantom, "\circlearrowleft"] & C_j \arrow[d, "h_j"] \\ D_i \arrow[r, "g_{ij}"] & D_j \end{tikzcd}$$

↳ This actually defines the category of direct systems!

Given a module M, define the constant direct system over I, $|M|$ as as

$$(\{M_i\}, \{f_{ij}\}) \;, \; M_i = M \;, \; f_{ij} = 1_M \; \forall i,j$$

$$\mathrm{Hom}_{\underline{RMod}}(\varinjlim_i C_i, M) = \mathrm{Hom}\big((\{C_i\},\{f_{ij}\}), |M|\big)$$

in the category of direct systems over I.

↳ Simply by univ. property of $\varinjlim_i C_i$!

§ 4.a Field theory

November-03-10
9:45 AM

Let us list some basic properties of fields. If F, K are fields:

* Either $\mathrm{Hom}(F,K) = \emptyset$ or every element of $\mathrm{Hom}(F,K)$ is injective.

  ↳ Because $\forall f \in \mathrm{Hom}(F,K)$, $\ker f \triangleleft F$, and the only ideals of a field are $\{0\}$ and $F \Rightarrow \ker f \in \{\{0\}, F\}$.

* If $F \subseteq K$, $\mathrm{Aut}_F(K)$ is a group,
  $\mathrm{Aut}_F(K) = \{\varphi : K \to K \text{ auto'} \text{ s.t. } \varphi|_F = id\}$

* If $F \subseteq K$, K is a v.sp. over F and we set $\dim_F(K) =: [K:F]$.

<u>Proposition</u>: If $F \subseteq L \subseteq K$ are fields,

$$[K:F] = [K:L][L:F]$$

<u>Proof</u> (sketch):

Take $\{\alpha_i\}_{i \in I}$ a basis for L over F and $\{\beta_j\}_{j \in J}$ a basis for K over L.

Prove that $\{\alpha_i \beta_j\}_{i,j}$ is a basis for K over F implying that

$$[K:F] = |I \times J| = |I| \times |J| = [K:L][L:F]$$

□

<u>Notation</u>: Istead of writing "K over F" we will write K/F, although this is a horrible abuse of notation.

N.B. K/F has nothing to do with a quotient!

* Let $f \in F[x]$ be an irreducible, non-constant poly., then if

$$K := F[x]/\langle f \rangle \leftarrow \text{quotient!}$$

K is a field, $F \subseteq K$, and $f(t)$ has a root in K, namely the coset of x.

Moreover, $[K:F] = \deg f$.

* $\exists$ canonical homo $\mathbb{Z} \to F$, $1 \mapsto 1$, extended by field operations.

* If this homo is injective, then $\mathbb{Z} \hookrightarrow F \overset{!}{\Longrightarrow} \mathbb{Q} \cong F$.

<u>Def</u>: In that case, we say that F has characteristic 0, and that $\mathbb{Q}$ is its prime field.

* Otherwise, the kernel of the canonical homo is an ideal of $\mathbb{Z}$. As $\mathbb{Z}$ is a PID, kernel $= (n) \triangleleft \mathbb{Z}$, since $\mathbb{Z}$ is an ID, $\mathbb{Z}/(n) \hookrightarrow F \Longrightarrow n = p$, prime.

Def: In that case, $\mathbb{Z}/p\mathbb{Z} \hookrightarrow F$ is called the prime field of F, which is given characteristic p.

Remark: If the field F is finite, it must have characteristic $p \implies$

$$\mathbb{Z}/p\mathbb{Z} \hookrightarrow F$$

$\implies \mathbb{Z}/p\mathbb{Z}$ is a subfield of $F \implies$

$\implies F$ is a vector space over $\mathbb{Z}/p\mathbb{Z}$

$\implies |F| = p^{\dim_{\mathbb{Z}/p\mathbb{Z}}(F)} = p^m$ for some $m \geq 1$.

Lemma: Gauss lemma.

Let R be a PID, Q its quotient ring. A monic poly $f \in R[x]$ is irreducible in $R[x]$ iff it is irreducible in $Q[x]$.

Proof: Exercise.

$\hookrightarrow$ Hint: The proof for a general R is identical to the one for $R = \mathbb{Z}$, $Q = \mathbb{Q}$.

Proposition: Eisenstein's criterion

Let R be a PID, $f \in R[x]$ a monic poly, of degree $d \geq 1$.

$$f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_1 x + a_0$$

Suppose $\exists$ prime p s.t. $\forall i$, $p \mid a_i$, but $p^2 \nmid a_0$, then f is irreducible over R.

Proof: Suppose $f = g \cdot h$ for $g, h \in R[x]$. Since f is monic, WLOG assume $\deg(g), \deg(h) > 0$ & both are monic.

$$g(x) = x^n + b_{n-1}x^{n-1} + \dots + b_1 x + b_0$$
$$h(x) = x^{d-n} + \dots + c_1 x + c_0$$

Consider $f = gh$ over $R/(p)[x]$, we get

$$\overline{f(x)} = x^d = \overline{g(x)} \cdot \overline{h(x)}$$

In a PID, p is prime $\Leftrightarrow$ (p) is prime $\Leftrightarrow$ $\Leftrightarrow$ (p) is maximal, so that $R/(p)$ is a field! Therefore, we get unique factorization in $R/(p)[x]$. By uniqueness,

$$\overline{g(x)} = x^n, \quad \overline{h(x)} = x^{d-n}, \text{ and so,}$$

$$(p \mid b_i \ \forall i) \ \& \ (p \mid c_i \ \forall i) \Longrightarrow p^2 \mid b_0 c_0 = a_0$$

$\times\!\!\!\times$

Field extensions

November-27-10
1:24 PM

Def: F, K fields, $F \subseteq K$ and $\{\alpha_i\}_{i\in I} \subseteq K$.
Then we define

$$F(\{\alpha_i : i \in I\}) = \bigcap_{F \subseteq K' \subseteq K} K'$$

where the intersection runs over all fields K', $F \subseteq K' \subseteq K$, s.t. $\{\alpha_i\}_{i\in I} \subseteq K'$.

$F(\{\alpha_i\}_I)$ is the minimal subfield of K containing F and all $\{\alpha_i\}_{i\in I}$.

Theorem: Let $f \in F[x]$ be an irreducible monic polynomial. Suppose $K \supseteq F$ is a field, where f has a root α. Then

1. $F[x]/(f(x)) \cong F(\alpha)$ via $\bar{x} \longmapsto \alpha$
2. Any non-zero polynomial $g \in F[x]$ with root α is a multiple of f.
3. $[F(\alpha) : F] = \deg f$

Def: Such f is called the minimal polynomial of α, and we set

$$\deg(\alpha) := \deg(f)$$

Proof: Define $\psi : F[x] \to K$ by $\begin{cases} \text{id on } F \\ x \mapsto \alpha \end{cases}$

As $f(x) \overset{\psi}{\longmapsto} f(\alpha) = 0$, we have that

$$\underbrace{F[x]/(f(x))}_{\text{this is a field, so the map must be injective}} \xrightarrow{\varphi} K$$

$\therefore F[x]/(f(x)) \overset{\varphi}{\hookrightarrow} K \implies F \cup \{\alpha\} \subseteq \overbrace{\operatorname{Im}\varphi}^{\text{a field}}$

$\implies F(\alpha) \subseteq \operatorname{Im}\varphi$ by minimality.

On the other hand, every element of $\operatorname{Im}\varphi$ has the form $\sum a_i\alpha^i \in F[x] \implies$

$\implies \operatorname{Im}\varphi \subseteq F(\alpha)$

$\therefore F[x]/(f(x)) \cong F(\alpha)$

And thus, $[F(\alpha):F] = [F[x]/(f(x)) : F] = \deg f$ ✓

Finally, say $g(\alpha) = 0$, $g \in F[x]$, $g \neq 0$, then $g \in \ker\psi \overset{!}{=} (f(x)) \implies f \mid g$ $\square$

Corollary: Any element of $F(\alpha)$ is of the form

$$\sum_i a_i\alpha^i, \quad a_i \in F$$

<u>Remark</u>: If each a_i satisfies a poly. over F,

$$F(\alpha_1,\dots,\alpha_{n+1}) = F(\alpha_1,\dots,\alpha_n)\,F(\alpha_{n+1})$$

$$\Longrightarrow F(\alpha_1,\dots,\alpha_n) = \Big\{ \sum_I a_I \alpha^I : a_I \in F \Big\}$$

where $I = (i_1,\dots,i_n)$, $\alpha^I = \alpha_1^{i_1}\cdots\alpha_n^{i_n}$.

<u>Theorem</u>: (Transport of structure)

Let $\varphi : F \to L$ be an iso' of fields, then φ induces an iso' $F[x] \overset{\sim}{\to} L[x]$.

Let f be an irreducible monic poly in $F[x]$, and ℓ its image under φ. Let $K_F \supseteq F$, $K_L \supseteq L$ be fields and α_F, α_L roots of f in K_F and ℓ in K_L resp. Then $\exists$ iso'

$$F(\alpha_L) \cong L(\alpha_L)$$

extending φ.

<u>Proof</u>:

$$\begin{aligned} F(\alpha_F) &\cong F[x]/(f(x)) \\ &\quad \downarrow \text{iso induced by } \varphi \\ L(\alpha_L) &\cong L[x]/(\ell(x)) \end{aligned}$$

$\square$

Proposition: Let $F \subseteq K$ be fields; $\alpha_1, \dots, \alpha_r \in K$ s.t. $\forall i$, $\deg(\alpha_i) = n_i$ (degree over F).

Then $[F(\alpha_1, \dots, \alpha_r) : F] \leq n_1 \cdots n_r$

Proof: By induction on r.

* The case $r = 1$ is clear.
* Assume for $(r-1)$, then

$$[F(\alpha_1, \dots, \alpha_r) : F] = [\overbrace{F(\alpha_1, \dots, \alpha_{r-1})}^{=L} F(\alpha_r) : F] =$$

$$= [F(\alpha_1, \dots, \alpha_r) : L][L : F]$$

Suppose α_r satisfies a monic irreducible poly $f \in F[x]$, then it will also satisfy a monic irreducible $g \in L[x]$, $g | f$

$$\Rightarrow \dots \leq n_1 \cdots n_{r-1} \cdot [L : F] \leq$$

$$\leq n_1 \cdots n_{r-1} \cdot \deg(g) \leq n_1 \cdots n_r$$

b/c $\deg(g) \leq \deg(f)$

$\square$

Def: Let K be a field, $K_1, K_2 \subseteq K$ subfields. The compositum $K_1 K_2$ is the minimal subfield of K containing both K_1 & K_2.

Example: $F \subseteq K$ fields, $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s \in K$,
$K_1 = F(\alpha_1, \dots, \alpha_r)$, $K_2 = F(\beta_1, \dots, \beta_s)$,

then $K_1 K_2 = F(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s)$.

Lemma: Let K, K_1, K_2 and F be as in the example above. Let
$\{\alpha_1, \dots, \alpha_n\}$ be a basis for K_1/F.
$\{\beta_1, \dots, \beta_m\}$ be a basis for K_2/F.

We claim that $\{\alpha_i \beta_j : 1 \le i \le n, 1 \le j \le m\}$ spans $K_1 K_2 / F$.

Proof: Let $X = \{\sum_{i,j} a_{ij} \alpha_i \beta_j : a_{ij} \in F, i \le n, j \le m\} \subseteq$

$\subseteq \{\sum_{I,J} a_{I,J} \alpha^I \beta^J : a_{I,J} \in F\} \overset{!}{=} K_1 K_2$,

where $I = (i_1, \dots, i_n)$, $J = (j_1, \dots, j_m)$, $\alpha^I = \alpha_1^{i_1} \cdots \alpha_n^{i_n}$

By minimality of $K_1 K_2$, to show $X = K_1 K_2$, it is enough to prove that
* X is closed under addition
* X is closed under multiplication
* $K_1 \cup K_2 \subseteq X$.

Then, by repeated addition and multiplication, each $\sum_{I,J} a_{I,J} \alpha^I \beta^J \in X \Rightarrow K_1 K_2 \subseteq X$.

So, first, closedness under addition is clear from the definition of X.

To prove that X is closed under multiplication, by linearity it is enough to show that for arbitrary $1 \le i,k \le n$, $1 \le j,l \le m$,

$$\alpha_i \beta_j \alpha_k \beta_l \in X$$

But as $\alpha_i \alpha_k \in K_1$, $\alpha_i \alpha_k = \sum_\mu a_\mu \alpha_\mu$, $a_\mu \in F$

$\beta_j \beta_l \in K_2$, $\beta_j \beta_l = \sum_\nu b_\nu \beta_\nu$, $b_\nu \in F$

$$\Longrightarrow \alpha_i \beta_j \alpha_k \beta_l = \left(\sum_\mu a_\mu \alpha_\mu\right)\left(\sum_\nu b_\nu \beta_\nu\right) =$$

$$= \sum_{\mu,\nu} (a_\mu b_\nu)\, \alpha_\mu \beta_\nu \in X$$

Now, if $f \in K_1$, $f = f \cdot 1$, $1 \in K_2 \Longrightarrow$

$$f = \left(\sum_i a_i \alpha_i\right)\left(\sum_j b_j \beta_j\right) = \sum_{i,j} (a_i b_j)\, \alpha_i \beta_j \in X$$

By symmetry, $K_2 \subseteq X$ too $\Longrightarrow K_1 \cup K_2 \subseteq X$.

□

<u>Theorem</u>: Suppose, as in the example above

$$\begin{tikzcd} & K & \\ K_1 \arrow[ur, dash] & & K_2 \arrow[ul, dash] \\ & F \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

with $[K_i : F] < \infty$, $i = 1,2$.

Then $[K_1 K_2 : F] \le [K_1 : F][K_2 : F]$, with equality iff a basis of K_2/F remains lin. indep. in K_2/K_1. In that case, it becomes a basis for $K_1 K_2 / K_1$.

<u>Proof of Theorem</u>: As in the statement of the lemma, let $\{\alpha_1, \dots, \alpha_n\}$, $\{\beta_1, \dots, \beta_m\}$ be bases for K_1/F, K_2/F resp.

Then $\{\alpha_i \beta_j\}_{i,j}$ spans K_1K_2/F and so, $\{\beta_j\}_j$ spans K_1K_2/K_1.

$\therefore$ $\{\beta_j\}_j$ form a basis iff they are lin. indep. over K_1.

$$[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : F] \leq$$

$$\leq m[K_1 : F] = [K_2 : F][K_1 : F]$$

with equality iff $\{\beta_j\}$ are lin. indep. over K_1.

$\square$

<u>Corollary</u>: If $\gcd([K_1 : F], [K_2 : F]) = 1$, then

$$[K_1K_2 : F] = [K_1 : F][K_2 : F]$$

<u>Proof</u>: In the case $K = K_1K_2$,
$$\begin{tikzcd}[column sep=small] & K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\ K_1 \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\ & F & \end{tikzcd},$$
$[K_1 : F] \mid [K_1K_2 : F]$ and $[K_2 : F] \mid [K_1K_2 : F]$, so since $\gcd = 1$,

$$[K_1 : F][K_2 : F] \mid [K_1K_2 : F]$$

On the other hand, $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$ by theorem, so we get equality.

$\square$

Example

$$f(x) = x^3 - 2 \quad \text{over } \mathbb{Q}$$

$\hookrightarrow$ irreducible by Eisenstein.

$$\Longrightarrow \quad
\begin{tikzcd}
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash, "3"] & \cong \ \mathbb{Q}(\omega\sqrt[3]{2}) \ \cong \arrow[d, dash, "3"] & \mathbb{Q}(\omega^2\sqrt[3]{2}) \arrow[dl, dash, "3"'] \\
& \mathbb{Q} &
\end{tikzcd}$$

order 3 $\longrightarrow$

where $\omega = e^{\frac{2\pi i}{3}} \in \mathbb{C}$, but then

$$\begin{tikzcd}
& K := \mathbb{Q}[\omega, \sqrt[3]{2}] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash, "3"] & \mathbb{Q}(\omega \cdot \sqrt[3]{2}) \arrow[d, dash, "3"] & \mathbb{Q}(\omega^2\sqrt[3]{2}) \arrow[dl, dash, "3"'] \\
& \mathbb{Q} &
\end{tikzcd}$$

In fact, $\mathbb{Q}[\omega, \sqrt[3]{2}]$ is the compositum of any two of the intermediate fields.

$$\mathbb{Q}[\sqrt[3]{2}] \cdot \mathbb{Q}[\omega \cdot \sqrt[3]{2}] = \mathbb{Q}[\sqrt[3]{2}, \omega \cdot \sqrt[3]{2}] \ni \omega$$
$$\Longrightarrow (= K.)$$

But $[K : \mathbb{Q}] \neq 9$ (although ≤ 9). In fact,

$$[K : \mathbb{Q}] = 6.$$

To see this consider $\mathbb{Q}(\omega) \cong \mathbb{Q}[x]/_{x^2+x+1}$ of degree 2 over $\mathbb{Q}$.

ω solves $x^3 - 1 = (x-1)(x^2+x+1)$.

irred. b/c roots are $\frac{-1 \pm \sqrt{-3}}{2}$

$K = \mathbb{Q}(\omega)\mathbb{Q}(\sqrt[3]{2}) \Longrightarrow$

$\Longrightarrow [K:\mathbb{Q}] = 2 \cdot 3 = 6$

by corollary as $(2,3) = 1$ ✓

§ 4.b Algebraic field extensions

November-05-10
9:49 AM

<u>Def</u>: $F \subseteq K$ fields, $\alpha \in K$ is algebraic over F if α satisfies a non-zero poly $f \in F[x]$
WLOG, f monic, irred.

Then, we have seen $F(\alpha) \cong F[x]/(f(x))$,

f = min. poly. of α over F
$\deg(\alpha) = \deg(f) = [F(\alpha):F]$

$\hookrightarrow$ f is the unique irred. poly. over F that α satisfies.

If α is NOT algebraic over F, then α is called transcendental over F.

<u>Proposition</u>: If α is transcendental over F, then

$$F(\alpha) \underset{F}{\cong} F(X) = \left\{ \frac{f(x)}{g(x)},\ g(x) \neq 0 \right\} = \mathrm{Frac}(F[x])$$

<u>Proof</u>: We have

$$F[x] \longrightarrow K \quad \text{via} \quad \begin{cases} F \ni a \longmapsto a \\ x \longmapsto \alpha \end{cases}$$

This ring homo is injective (if $f(x) \in \ker$, $f(\alpha) = 0$ ✳).

By univ. property

$F(X) \hookrightarrow K$. Call L the image, $\alpha \in L$
$\Rightarrow L \supseteq F(\alpha)$

OTOH, $L = \left\{ \frac{f(\alpha)}{g(\alpha)}, g(x) \neq 0 \right\} \subseteq F(\alpha)$

$\therefore F(X) \cong L = F(\alpha)$

$\square$

Proposition: $F \subseteq K$, $\alpha \in K$, then

$[F(\alpha) : F] < \infty \iff \alpha$ is alg. over F

Proof: α alg. $\Rightarrow [F(\alpha) : F] = \deg(\alpha) < \infty$

If α is not alg. (transcendental), then

$[F(\alpha) : F] = [F(X) : F] \geq [F[x] : F] = \infty$

(or more precisely $\aleph_0$ (aleph 0).)

Alternately, if $[F(\alpha) : F] < \infty$, then for some first n, $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ must be lin. dep. over F

$\Rightarrow \exists \sum q_i \alpha^i = 0 \Rightarrow \alpha$ solves $\sum q_i \alpha^i$

$\square$

Theorem: Let $F \subseteq K$ be fields, let $H = \{\alpha \in K : \alpha \text{ is alg. over } F\}$.

Then H is a field, $F \subseteq H \subseteq K$; any element in $K \setminus H$ is transcendental **over H** (so also over F).

We call such H the algebraic closure of F in K.

Proof: First $H \supseteq F \Rightarrow$ any $\alpha \in F$ solves $x - \alpha \in F[x]$.

Need to show that H is closed under field operations $+, -, \times, (\cdot)^{-1}$, i.e. if $\alpha, \beta \in H$ $\alpha+\beta, -\alpha, \alpha\beta$ & $1/\alpha \in H$. (if $\alpha \neq 0$).

If $\gamma \in \{\alpha+\beta, -\alpha, \alpha\beta, \frac{1}{\alpha}\}$, then enough

$$[F(\gamma) : F] < \infty$$

Note $F(\alpha,\beta) \supseteq F(\gamma) \supset F$, so

$$[F(\gamma):F] \leq [F(\alpha,\beta):F] \leq [F(\alpha):F][F(\beta):F] < \infty \checkmark$$

To show $\alpha \in K \setminus H$ is transcendental over H, equiv. if α is alg. over H, $\alpha \in H$, i.e. sp. $\exists f$

$f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0$, $a_i \in H$ that α solves

$\Longrightarrow$ α algebraic over $F(a_0, a_1, \dots, a_{d-1})$

$$[F(\alpha):F] \leq [F(a_0, \dots, a_{d-1}, \alpha):F] \leq$$

$$\leq [F(a_0, \dots, a_{d-1}, \alpha):F(a_0, \dots, a_{d-1})]\,[F(a_0, \dots, a_{d-1}):F] \leq$$

$$\leq d \cdot \prod_{i=0}^{d-1} [F(a_i):F] < \infty$$

$\Longrightarrow$ α is alg. over $F \Longrightarrow \alpha \in H$.

$\square$

<u>Corollary</u> (of the proof): $L \supseteq K \supseteq F$ fields s.t.

* L/K is an algebraic extension, i.e. any $\ell \in L$, is algebraic over K.
* K/F is an algebraic extension.

Then L/F is an algebraic extension.

<u>Def</u>: L/K is called a purely transcendental extension if the algebraic closure of K in L is K itself.

<u>Exercise</u>: $K(x)/K$ is purely transcendental.

$\hookrightarrow$ Recall that $K(x) = \mathrm{Frac}(K[x]) =$

$$= \left\{ \frac{f(x)}{g(x)} : f, g \in K[x],\ g \neq 0 \right\}$$

Corollary: $F \subseteq K$ has this structure

$$\begin{tikzcd} K \arrow[d, dash, "\text{purely trans. extension}"] \\ H \arrow[d, dash, "\text{algebraic extension}"'] \\ F \end{tikzcd}$$

Def. A field K is called *algebraically closed* if any non-constant $f(x) \in K[x]$ has a root in K.

Equivalently, every such f splits into linear terms over K.

Def. Let $F \subseteq K$ be fields, then K is called an *algebraic closure* of F if:

* K over F is an algebraic extension
* $\forall f \in F[x]$ has a root in K. (or, equivalently, splits into linear terms over K).

Proposition: If K is an algebraic closure of F, then K is algebraically closed.

Proof: Let $f(x) \in K[x]$, a non-const. poly. Then let $\alpha \in K_1 \supseteq K$ be a root of f (such α exists).

$$K_1 \supseteq \underbrace{K(\alpha) \supseteq \bar{K}}_{\text{algebraic}} \underbrace{\supseteq K}_{\text{algebraic}} \implies \text{By a previous result}$$

$\implies K(\alpha) \supseteq F$ is also algebraic

$\implies \alpha$ solves some $g(x) \in F[x]$, $g(x) \neq 0$, monic.

Over $\bar{K}$, $g(x) = \prod_{i=1}^{d} (x - \alpha_i)$

$g(\alpha) = 0 \implies \alpha = \alpha_{i_0}$ for some $1 \leq i_0 \leq d$, and so, $\alpha \in \bar{K}$.

$\square$

<u>Theorem</u>: Any field F has an algebraic closure K. Moreover, if K_1 is another alg. closure, then

$$K_1 \underset{F}{\cong} K$$

↳ The notation for this K is usually $\bar{F}$ or F^{alg}.

<u>Proof</u>: See Dummit & Foote $\square$

<u>Rmk</u>: In almost any case, we have no idea what $\bar{F}$ looks like.

<u>Exceptions</u>: $F =$ finite field

$F = \mathbb{R}, \mathbb{C} \implies \bar{F} = \mathbb{C}$;

$F = \mathbb{Q}$ is a big MYSTERY!

Splitting fields

November-08-10
9:53 AM

Let F be a field, $f(x) \in F[x]$ a polynomial, irreducible or not.

Def: A field $K \supseteq F$ is called a splitting field of f if over K,

$$f(x) = c \cdot \prod_{i=1}^{d} (x - \alpha_i) \quad , \alpha_i \in K.$$

and $K = F(\alpha_1, \dots, \alpha_d)$.

Theorem: If both K_1 & K_2 are splitting fields for f, then $\exists$ iso

$$K_1 \overset{\varphi}{\underset{F}{\cong}} K_2 \quad (\varphi|_F = id)$$

Proof: We will show that if F, L are fields, $\varphi : F \to L$ an iso and $\varphi_* : F[x] \to L[x]$, the induced iso, then if

$$\begin{cases} K_F \text{ is a splitting field for } f(x) \\ K_L \text{ is a splitting field for } \ell(x) = \varphi_*(f(x)) \end{cases}$$

Then $\exists$ iso $\psi : K_F \to K_L$ extending φ, i.e. s.t.

$$\begin{array}{ccc} K_F & \xrightarrow{\psi} & K_L \\ \cup\!\! \mid & \circlearrowleft & \cup\!\! \mid \\ F & \xrightarrow{\varphi} & L \end{array}$$

We will show that by induction on $\deg(f)$. Let $f_1(x) \mid f(x)$ be an irreducible factor, and

$$\ell_1(x) \mid \ell(x), \quad \ell_1(x) = \varphi_*(f_1(x))$$

Let α_F be a root of $f_1(x)$ in K_F
α_L be a root of $\ell_1(x)$ in K_L

Then, by a previous result, $\exists$ iso $\tilde{\varphi}: F(\alpha_F) \to L(\alpha_L)$ extending φ s.t. $\tilde{\varphi}(\alpha_F) = \alpha_L$

$$\begin{array}{ccc} K_F & & K_L \\ | & & | \\ F(\alpha_F) & \xrightarrow{\tilde{\varphi}} & L(\alpha_L) \\ | & & | \\ F & \xrightarrow{\varphi} & L \end{array}$$

Over $F(\alpha_F)$, we have

$$\tilde{f}(x) = \frac{f(x)}{(x-\alpha_F)}$$

Over $L(\alpha_L)$, $\tilde{\ell}(x) = \dfrac{\ell(x)}{(x-\alpha_L)} \overset{!}{=} \varphi_*(\tilde{f}(x))$.
Moreover, we still have that

$$\begin{cases} K_F \text{ is the splitting field of } \tilde{f} \text{ over } F(\alpha_F) \\ K_L \text{ is the splitting field of } \tilde{\ell} \text{ over } L(\alpha_L). \end{cases}$$

$\therefore$ By induction hypothesis, as
$$\deg(\tilde{f}) \leq \deg(f) - 1 < \deg(f),$$
we obtain the iso ψ extending $\tilde{\varphi}$, and therefore extending φ as well, s.t.

$$K_F \overset{\psi}{\cong} K_L.$$

$\square$

Proposition: $f \in F[x]$, then $\exists$ a splitting field K for f s.t.

$$[K:F] \leq d! \quad , d = \deg(f).$$

Proof (Sketch): By induction on d,

1. Show that $\exists K_1$, $[K_1 : F] < d$, $K_1 = F(\alpha)$ for some root α of f.

e.g. If $f_1 | f$ is an irreducible factor, then we could take

$$K_1 = F[x] / (f_1(x))$$

2. Over K_1, we are dealing with $\frac{f(x)}{x - \alpha} \Longrightarrow$ Apply induction.

$\square$

§ 4.c Examples: finite and cyclotomic fields

November-27-10
5:58 PM

We will analyze two examples of splitting fields:

1. Finite fields
2. Cyclotomic fields

They will turn out to be useful later on in the context of Galois theory.

Example 1: Finite fields.

Lemma: Let F be a finite field with q elements. Then $F^{\times} = F \setminus \{0\}$ is a cyclic group with $q-1$ elements, under multiplication.

Proof: Exercise.

Theorem: (Everything you wanted to know about finite fields, but were afraid to ask)

Let p be a prime and $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$, a finite field with p elements.

If $\overline{\mathbb{F}}$ is an algebraic closure of $\mathbb{F}$, then

① $\forall m \in \mathbb{N}$, $m \geq 1$, $\overline{\mathbb{F}}$ contains a unique subfield with p^m elements, denoted by $\mathbb{F}_{p^m}$, and

$$\mathbb{F}_{p^m} = \{ \alpha \in \overline{\mathbb{F}} : \alpha^{p^m} - \alpha = 0 \}$$

② $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ iff $m \mid n$. Therefore, the lattice of finite subfields of $\overline{\mathbb{F}}$ is opposite to the lattice of finite subgroups of $\mathbb{Z}$, via $\mathbb{F}_{p^m} \longleftrightarrow m\mathbb{Z}$.

That is $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m\mathbb{Z} \supseteq n\mathbb{Z}$,
$\mathbb{F}_{p^m} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^{(m,n)}} \iff m\mathbb{Z} + n\mathbb{Z} = (m,n)\mathbb{Z}$,
$\mathbb{F}_{p^m} \cdot \mathbb{F}_{p^n} = \mathbb{F}_{p^{\mathrm{lcm}(m,n)}} \iff m\mathbb{Z} \cap n\mathbb{Z} = \mathrm{lcm}(m,n)\mathbb{Z}$

③ Let $f \in \mathbb{F}_{p^m}[x]$ be irreducible of degree n, and let $\alpha \in \overline{\mathbb{F}}$ be a root of f. Then

$\mathbb{F}_{p^m}(\alpha) = \mathbb{F}_{p^{n \cdot m}}$ and is the splitting field of f.

④ Let L be any field with p^m elements, then

$$L \cong \mathbb{F}_{p^m}$$

⑤ $\overline{\mathbb{F}}$ is an algebraic closure of $\mathbb{F}_{p^m}$.

⑥ The Frobenius map $\mathrm{Fr}_{p^m} : \overline{\mathbb{F}} \to \overline{\mathbb{F}}$, $x \longmapsto x^{p^m}$ is a field auto' of $\overline{\mathbb{F}}$, whose fixed points are precisely $\mathbb{F}_{p^m}$.

⑦ $\overline{\mathbb{F}} = \bigcup_{m=1}^{\infty} \mathbb{F}_{p^m}$.

Proof: (1) Suppose L is a finite subfield of $\overline{\mathbb{F}}$. Let M be its prime subfield. Then $|M| = p$ (by def. of prime subfield), and $[L:M] = m$. Then $|L| = p^m$ and so, by lemma, $L^\times$ is a cyclic group with $p^m - 1$ elements; thus,

$$L^\times \subseteq \{ a \in \overline{\mathbb{F}} : a^{p^m - 1} = 1 \} \Rightarrow$$

$$\Rightarrow L^\times \subseteq \{ a \in \overline{\mathbb{F}} : a \text{ solves } \underbrace{x^{p^m-1} - 1 = 0}_{\text{has atmost } p^m - 1 \text{ roots}} \}$$

$$\Rightarrow L = \{ a \in \overline{\mathbb{F}} : a^{p^m} = a \}$$

$$\Rightarrow L \text{ is unique (given } m).$$

Conversely, given m, let

$$L := \{ a \in \overline{\mathbb{F}} : a^{p^m} = a \} =$$

$$= \{0\} \cup \{ a \in \overline{\mathbb{F}} : a \text{ solves } \overbrace{x^{p^m-1} - 1}^{=: f(x)} = 0 \}$$

As $\gcd(f, f') = \gcd(x^{p^m-1} - 1, (p^m - 1) x^{p^m - 2}) = 1$, in $\overline{\mathbb{F}}$, f is separable, i.e. has $(p^m - 1)$ distinct roots.

$$\Rightarrow |L| = p^m$$

Clearly, $\forall x, y \in L$, $xy \in L$; $0, 1 \in L$; $x \neq 0 \Rightarrow \frac{1}{x} \in L$; and $-x \in L$, because $(-1)^{p^m} = -1$ (?)

Also, as $(x+y)^p = x^p + y^p + \sum_{1}^{p-1} \binom{p}{i} x^{p-i} y^i$ and $\forall$ prime p, $p \mid \binom{p}{i}$ $\forall 1 \leq i \leq p-1$,

$$(x+y)^p \equiv x^p + y^p \mod p.$$

$\Rightarrow$ in $\overline{\mathbb{F}}/\mathbb{F}$, $(x+y)^{p^m} = x^{p^m} + y^{p^m}$ $\forall x,y \in \overline{\mathbb{F}}$, $m \geq 0$.

So that, L is closed under addition $\Rightarrow$
$\Rightarrow L$ is a subfield of $\overline{\mathbb{F}}$. ✓

---

② If $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, $\mathbb{F}_{p^n}$ is a vector space over $\mathbb{F}_{p^m}$. So, $|\mathbb{F}_{p^n}| = p^n = |\mathbb{F}_{p^m}|^a = p^{ma}$ for some a.

$$\Longrightarrow m \mid n$$

Conversely, if $m \mid n$, say $n = mb$, then

$$\left(x^{p^m} = x\right) \longrightarrow x^{p^{2m}} = \left(x^{p^m}\right)^{p^m} = x^{p^m} = x$$

Reating b times, $x^{p^n} = x^{p^{bm}} = x$.

As $\begin{cases} \mathbb{F}_{p^m} = \{a \in \overline{\mathbb{F}} : a^{p^m} = a\} \\ \mathbb{F}_{p^n} = \{a \in \overline{\mathbb{F}} : a^{p^n} = a\} \end{cases} \Longrightarrow \mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ ✓

Also, $\mathbb{F}_{p^m} \cap \mathbb{F}_{p^n}$ is a finite subfield of $\overline{\mathbb{F}}$ $\Rightarrow$
$\mathbb{F}_{p^m} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^t}$ for some t. As $\mathbb{F}_{p^t} \leq \mathbb{F}_{p^m}$, $t \mid m$ and so $t \mid n$ too $\Rightarrow$ maximal such $t = (m,n)$

Similarly, $\mathbb{F}_{p^m}\mathbb{F}_{p^n} = \mathbb{F}_{p^t}$, $m \mid t$ & $n \mid t$
$\Rightarrow$ minimal such $t = \operatorname{lcm}(m,n)$. ✓

---

③ We already know that

$$\mathbb{F}_{p^m}(\alpha) = \mathbb{F}_{p^m}[x] \big/ (f(x))$$ ← v. sp. of dimension n over $\mathbb{F}_{p^m}$

$$\Longrightarrow |\mathbb{F}_{p^m}(\alpha)| = (p^m)^n = p^{mn}.$$

Therefore by uniqueness of subfields,

$$\mathbb{F}_{p^m}(\alpha) = \mathbb{F}_{p^{mn}}.$$

Since this is true for all roots α of f and the RHS is independent of α, f splits over $\mathbb{F}_{p^{mn}}$. As α is a root of f, $\mathbb{F}_{p^m}(\alpha)$ must be contained in the splitting field, so $\mathbb{F}_{p^m}$ is the splitting field.

---

④ We saw that $L^\times$ is a cyclic group with $p^m - 1$ elements $\Longrightarrow L$ is a splitting field for $x^{p^m} - x \in M[x]$, where M is the prime subfield of L, $|M| = p$.
It is easy to see that $|M| = p \Longrightarrow M \cong \mathbb{F}_p$

On the other hand, $\mathbb{F}_{p^m}$ is the splitting field for $x^{p^m} - x \in \mathbb{F}_p[x]$, so

$$\begin{array}{ccc} L & & \mathbb{F}_{p^m} \\ | & & | \\ M & \cong & \mathbb{F}_p \end{array} \Longrightarrow$$ By a theorem about splitting fields,

$$L \cong \mathbb{F}_{p^m}$$

---

(5) Let $f \in \mathbb{F}_{p^m}[x]$. Since $\overline{\mathbb{F}}$ is algebraically closed, f splits over $\overline{\mathbb{F}}$.
On the other hand every element of $\overline{\mathbb{F}}$ is algebraic over $\mathbb{F}_p \Longrightarrow$ over $\mathbb{F}_{p^m}$ too ✓

---

(6), (7) We already saw that in $\mathbb{F}$,

$$\begin{aligned} (x+y)^p &= x^p + y^p \\ (xy)^p &= x^p y^p \\ 1^p &= 1 \end{aligned}$$

$\Longrightarrow Fr_p$ is a field homo', and thus must be injective (b/c $\ker Fr_p \neq \overline{\mathbb{F}}$).

Now, if $a \in \mathbb{F}_{p^m}$, then $a^p \in \mathbb{F}_{p^m}$ b/c $(a^{p^m} = a) \Longrightarrow \left[(a^p)^{p^m} = (a^{p^m})^p = a^p\right]$ ✓

Thus, $Fr_p(\mathbb{F}_{p^m}) \subseteq \mathbb{F}_{p^m} \Rightarrow Fr_p$ is also surjective as a map $\mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$. Therefore Fr_p is an auto' of $\mathbb{F}_{p^m}$ for every $m \geq 1$.

If $a \in \overline{\mathbb{F}}$, then a is algebraic over $\mathbb{F}_p \Longrightarrow$
$\Longrightarrow \mathbb{F}_p(a)$ is finite field $\Longrightarrow \mathbb{F}_p(a) = \mathbb{F}_{p^m}$ for some $m \geq 1$. $\Longrightarrow \overline{\mathbb{F}} = \bigcup_{m\geq 1} \mathbb{F}_{p^m}$ and proves (7)

Also, $\overline{\mathbb{F}} = \bigcup_{m\geq 1} \mathbb{F}_{p^m} \Longrightarrow Fr_p$ is an auto' of $\overline{\mathbb{F}}$.

Finally, as $Fr_{p^m} = \overbrace{Fr_p \circ \dots \circ Fr_p}^{m \text{ times}}$, we get our claim.

□

Example 2: Cyclotomic fields

Def: We define the Euler φ-function by

$$\varphi(1) = 1, \quad \varphi(n) = \#\{1 \le a \le n \mid (a,n) = 1\}$$

Notice that for any prime p,

$$\varphi(p^a) = p^a - p^{a-1} = p^a(1 - 1/p),$$

and that φ is multiplicative, i.e.

$$\varphi(nm) = \varphi(n)\varphi(m) \quad \text{if } (n,m) = 1$$

$$\therefore \varphi(n) = n \prod_{\substack{p \mid n \\ p\text{-prime}}} (1 - 1/p)$$

Set $\mu_n = \{z \in \mathbb{C} : z^n = 1\} = \{e^{\frac{2\pi i a}{n}} : 0 \le a < n\}$

$\hookrightarrow$ The n^{th} roots of unity — a multiplicative group of n elements, solutions of

$$z^n - 1 = 0 \quad \text{over } \mathbb{C}$$

Set $\mathbb{Q}(\mu_n)$ = splitting field of $z^n - 1 \in \mathbb{Q}[z]$

If $\zeta = e^{\frac{2\pi i}{n}}$, then $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$ via $\zeta^a \mapsto a$.

Since the generators of $\mathbb{Z}/n\mathbb{Z}$ are $\{a \le n \mid (a,n) = 1\}$, it follows that the generators of μ_n are the, so called, primitive n^{th} roots of unity

$$\{\zeta^a \mid (a,n) = 1\}$$

There are precisely $\varphi(n)$ of those.

Note $\mu_d \subseteq \mu_n \iff d \mid n$, and so,

$$\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta) = \mathbb{Q}(\zeta^a) \quad \forall (a,n)=1.$$

<u>Def</u>: The n^{th} cyclotomic polynomial Φ_n is

$$\Phi_n(x) = \prod_{\substack{\zeta \in \mu_n \\ \zeta \text{ primitive}}} (x-\zeta) = \prod_{\substack{(a,n)=1 \\ 1 \le a \le n}} (x-\zeta^a)$$

Since any $\alpha \in \mu_n$ is primitive of degree $\operatorname{ord}(\alpha) = d$ and $d \mid n$,

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

<u>Examples</u>:

$$\Phi_1(x) = x-1$$

$$\Phi_2(x) = \frac{x^2-1}{x-1} = x+1$$

$$\Phi_3(x) = \frac{x^3-1}{x-1} = x^2+x+1$$

$$\Phi_4(x) = \frac{x^4-1}{(x-1)(x+1)} = x^2+1$$

$$\Phi_5(x) = \frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1$$

$$\Phi_6(x) = \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)} = x^2-x+1$$

Proposition: $\Phi_n(x) \in \mathbb{Z}[x]$, $\deg(\Phi_n) = \varphi(n)$.

Proof: By induction on n, $n=1$ is clear

Given $n>1$, $f_n(x) := \prod_{\substack{d \mid n \\ d<n}} \Phi_d(x) \in \mathbb{Z}[x]$ monic (by ind. hyp.)

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

$f_n(x) \mid x^n - 1$ in $\mathbb{Q}[x]$, hence

in $\mathbb{Z}[x]$ (by Gauss Lemma).

Since $\Phi_n(x) = \dfrac{x^n-1}{f_n(x)}$, done! $\square$

Theorem: $\Phi_n(x)$ is irreducible over $\mathbb{Q}$

Proof: ζ_n solves $\Phi_n(x) \Rightarrow$ is algebraic $\Rightarrow$

$\Rightarrow$ Let $f_n(x)$ be the min. poly. of ζ_n over $\mathbb{Q}$.

Then, $f_n \mid \Phi_n$ in $\mathbb{Q}[x]$, and hence in $\mathbb{Z}[x]$.

It follows that $x^n - 1 = f_n(x)\, h(x)$, where both $f_n, h \in \mathbb{Z}[x]$, monic.

We will now show that if ζ is a root of f_n and p is a prime, $(p,n)=1$, then ζ^p is also a root of $f_n(x)$.

Since all primitive nth roots can be obtained by (repeatedly) sending $\zeta \mapsto \zeta^p$, they are all roots of $f_n \Rightarrow f_n = \Phi_n$ ✓

Suppose $f_n(\zeta) = 0$. If $f_n(\zeta^p) \neq 0$, then must have $h(\zeta^p) = 0 \Rightarrow$

$\Rightarrow \zeta^p$ solves $h(x) \Rightarrow \zeta$ solves $h(x^p)$.

Since f_n is the min. poly. of ANY of its roots (b/c irreducible!),

$$h(x^p) = f_n(x)\, g(x), \quad g \in \mathbb{Z}[x] \text{ (by Gauss)}.$$

Reduce mod p and denote $\bar{h}, \bar{f_n}, \bar{g}$ the reduction.

Trick! $\overline{h(x^p)} = \overline{h(x)}^p = \bar{f_n} \cdot \bar{g}$

b/c $\left(\sum a_i x^i\right)^p = \sum a_i^p (x^i)^p = \sum a_i (x^p)^i$

if $a_i \in$ Field of char $= p$ by Fermat's little theorem $a_i \in \mathbb{F}_p$

$\therefore \bar{f_n}$ & $\bar{h}^p$ (and hence $\bar{h}$) have a common root mod p. But

$$\bar{f_n} \cdot \bar{h} = \overline{x^n - 1},$$

and $x^n - 1$ is separable over $\mathbb{F}_p$, as

$$(nx^{n-1}, x^n - 1) = 1, \quad nx^{n-1} \neq 0 \text{ b/c } (p,n) = 1$$

$\Rightarrow f$ & h have no common roots.
Contradiction! $\square$

$\therefore \Phi_n(x) \in \mathbb{Z}[x]$, monic, irreducible, and has degree $\varphi(n)$.

Since $\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[x]/(\Phi_n(x)) \Rightarrow$
$\Rightarrow [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

<u>Corollary</u>: If $(n,m) = 1$, then
$$\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$$

<u>Note</u>: If $d|n, d|m$, $\mu_d \subseteq \mu_n \cap \mu_m$ and so,
$$\mathbb{Q}(\zeta_d) \subseteq \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m)$$
As $[\mathbb{Q}(\zeta_d) : \mathbb{Q}] = \varphi(d) = \prod_{p|d} (p^{a(p)} - p^{a(p)-1})$,
where $p^{a(p)}$ is the largest power of p dividing d,
$[\mathbb{Q}(\zeta_d) : \mathbb{Q}] = 1 \iff \underline{d = 1 \text{ or } 2}$

<u>Proof</u>: Notice that
$\mathbb{Q}(\zeta_{nm}) = \mathbb{Q}(\zeta_n) \cdot \mathbb{Q}(\zeta_m)$, b/c $\supseteq$ is clear, and $\subseteq$ is due to $\zeta_n \cdot \zeta_m$ is a primitive mn-root 1.

$$
\begin{tikzcd}
 & \mathbb{Q}(\zeta_{nm}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\zeta_m) \arrow[dr, dash, "\varphi(m)/a"] \arrow[ddr, dash, bend right, "\varphi(m)"'] & & \mathbb{Q}(\zeta_n) \arrow[dl, dash, "\varphi(n)/a"'] \arrow[ddl, dash, bend left, "\varphi(n)"] \\
 & K := \mathbb{Q}(\zeta_n)\cap\mathbb{Q}(\zeta_m) \arrow[d, dash, "a"] & \\
 & \mathbb{Q} &
\end{tikzcd}
$$

$$\varphi(n,m) = [\mathbb{Q}(\zeta_{nm}) : \mathbb{Q}] = a\,[\mathbb{Q}(\zeta_{nm} : K)] \leq$$

by compositant result

$$\leq a\,[\mathbb{Q}(\zeta_m):K][\mathbb{Q}(\zeta_n):K]$$

$$= a \cdot \frac{\varphi(m)}{a} \cdot \frac{\varphi(n)}{a}$$

b/c $(n,m)=1$

$$= \frac{\varphi(n,m)}{a} \implies \underline{a = 1}$$

$\square$

Rmk: One can show that if $d=(n,m)$,

$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d)$$

Note: $\forall\ (a,n)=1$, $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n^a)$, and both ζ_n & ζ_n^a are roots of $\Phi_n(x)$

One splitting field of Φ_n $\quad$ another splitting field of Φ_n

$$
\left\{\begin{tikzcd}
\mathbb{Q}(\zeta_n) \arrow[r, "\cong", "\varphi_a"'] \arrow[d, dash] & \mathbb{Q}(\zeta_n^a) \arrow[d, dash] \\
\mathbb{Q} \arrow[r, equal, "\mathrm{Id}"'] & \mathbb{Q}
\end{tikzcd}\right\}
$$

$\therefore\ \exists \varphi_a$ s.t. $\varphi \in \mathrm{Aut}(\mathbb{Q}(\zeta_n) \text{ over } \mathbb{Q})$,

$$\varphi_a(\zeta_n) = \zeta_n^a.$$

We therefore get a map

$$(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathrm{Aut}(\mathbb{Q}(\zeta_n) \text{ over } \mathbb{Q})$$

integers prime to n under mult.

$$a \longmapsto \varphi_a$$

The φ_a is determined by its effect on ζ_n, b/c

$$\mathbb{Q}(\zeta_n) = \left\{ \sum_{i=0}^{\varphi(n)-1} a_i \zeta_n^i : a_i \in \mathbb{Q} \right\}$$

Conclusion: $\mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathrm{Aut}(\mathbb{Q}(\zeta_n))$

group homo'

Finally, if $\varphi \in \mathrm{Aut}(\mathbb{Q}(\zeta_n))$, then $\varphi(\zeta_n)$ is an n'th root of unity of exact order n

$\Longrightarrow \exists a$ s.t.

$$\varphi(\zeta_n) = \zeta_n^a, \quad (a,n) = 1$$

$$\Longrightarrow \varphi = \varphi_a \Longrightarrow$$

$$\Longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times = \mathrm{Aut}(\mathbb{Q}(\zeta_n))$$

§ 4.d Galois theory

November-12-10
9:36 AM

K field, $\underbrace{\mathrm{Aut}(K)}_{\text{group under composition.}} = \{\varphi : K \to K \text{ bijective ring homo'}\}$

$K \supseteq F$ subfield,

$\mathrm{Aut}(K/F) \subseteq \mathrm{Aut}(K)$, subgroup.

$\mathrm{Aut}(K/F) = \{\varphi \in \mathrm{Aut}(K) \mid \varphi|_F = \mathrm{Id}_F\}$

If F is the prime field of K, then

$$\mathrm{Aut}(K) = \mathrm{Aut}(K/F)$$

<u>Proposition</u>: $K \supseteq F$, $\alpha \in K$ algebraic over F. Let f = min. poly. of α over F.
Then, for any $\varphi \in \mathrm{Aut}(K/F)$, $\varphi(\alpha)$ is also a root of f. One then obtains a homo'

$$\mathrm{Aut}(K/F) \longrightarrow \Sigma_T, \quad T = \{\text{roots of } f\}$$

<u>Proof</u>: Say $f(x) = x^d + \dots + a_1 x + a_0$, $a_i \in F$, $\varphi \in \mathrm{Aut}(K/F)$

$$0 = \varphi(0) = \varphi\left(\sum_{i=0}^{d} a_i \alpha^i\right) = \sum_{i=0}^{d} \varphi(a_i)\varphi(\alpha)^i \overset{\varphi|_F = \mathrm{Id}_F}{=}$$

$$= \sum_{0}^{d} a_i \varphi(\alpha)^i = f(\varphi(\alpha))$$

$\square$

Suppose $f(x) \in F[x]$ is an irreducible poly. and $F(\alpha)$ is a splitting field of f, where α is a root.

Then, $\forall$ other root β of f, we have

$$F(\alpha) = F(\beta)$$

$$\Big(\underbrace{\overbrace{F(\alpha) \supseteq F(\beta)}^{\deg f} \supseteq F}_{\deg f} \implies [F(\alpha) : F(\beta)] = 1 \Big)$$

On the other hand, by splitting fields thm, $\exists \varphi_\beta$ s.t.

$$\begin{tikzcd} F(\alpha) \arrow[r, "\sim", "\varphi_\beta"'] \arrow[d, dash] & F(\beta) \arrow[d, dash] \\ F \arrow[r, "Id"] & F \end{tikzcd} , \quad \varphi_\beta(\alpha) = \beta$$

Furthermore, φ_β is uniquely determined by $\varphi_\beta(\alpha) = \beta$.

Therefore, $|\mathrm{Aut}(F(\alpha)/F)| = \#$ of distinct roots of f in $F(\alpha)$

(*) if f is separable

$= \deg(f) = [F(\alpha) : F] =: n$ ✓

We also have, $\mathrm{Aut}(F(\alpha)/F) \longrightarrow S_n$, injective, the image is a subgroup with n elements, and is a transitive subgroup.

Example: Let F be a field, $\operatorname{ch} F = p$,

$$F(t) = \left\{ \frac{h(t)}{g(t)} ,\ h, g \in F[t],\ g \neq 0 \right\}$$

$$f(x) = x^p - t \in (F(t))[x]$$

f has a root in $F(t^{1/p})$ and there,

$$f(x) = (x - t^{1/p})^p \quad \text{(by bin. formula for } \operatorname{ch} F = p)$$

$\Longrightarrow$ f is irreducible over $F(t)$, not separable.

$\Longrightarrow$ $(*)$ is important

Examples:

(1) $F = \mathbb{Q}$, $K = \mathbb{Q}(\zeta_n)$

$$\operatorname{Aut}(K/F) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

(2) $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $K = \mathbb{F}_{p^m}$

Let $\zeta \in K^\times$ be a generator of this cyclic gp.
Let f be the min. poly. of ζ over $\mathbb{F}_p$.

Clearly, $\mathbb{F}_p(\zeta) = K$. If ζ' is another root of f in $\overline{\mathbb{F}_p}$, then

$$[\mathbb{F}_p(\zeta') : \mathbb{F}_p] = \deg(f) = [\mathbb{F}(\zeta) : \mathbb{F}_p] = m$$

$$\Longrightarrow \mathbb{F}_p(\zeta') = \mathbb{F}_{p^m} = K$$

$\therefore$ K is the splitting field of f.

Let $Fr : K \to K$, $Fr(a) = a^p$ be the Frobenius automorphism.

$$Fr \in \mathrm{Aut}(K/\mathbb{F}_p) \text{ \& has order } m$$

$$Fr^m(a) = a^{p^m}$$

$\Longrightarrow$ f is separable by (*) &

$$\mathrm{Aut}(K/\mathbb{F}_p) = \langle Fr \rangle$$ cyclic subgroup of order m

In fact, let $g(x) = \prod_{i=0}^{m-1} (x - \zeta^{p^i})$, $\deg(g) = m$ and $g(\zeta) = 0$.

On the other hand, applying Frobenius on the coefficients of g,

$$Fr(g(x)) = \prod_{i=0}^{m-1} (x - Fr(\zeta^{p^i})) =$$

$$= \prod_{i=0}^{m-1} (x - \zeta^{p^{i+1}}) = g(x) \text{ b/c } (\zeta^{p^m} = \zeta)$$

$\Longrightarrow$ $g(x)$ has coefficients in $\mathbb{F}_p$ (= fixed field of Fr)

$$\Longrightarrow \quad f(x) \mid g(x) \quad \xrightarrow{\uparrow} \quad f(x) = g(x)$$

by degree consideration

③ $F = \mathbb{Q}$, $f(x) = x^2 - 2$, $K = \mathbb{Q}(\sqrt{2})$

$\mathrm{Aut}(K/F) = \{1, \sigma\}$, $\sigma(\sqrt{2}) = -\sqrt{2}$.

④ $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$.

Although $f(x) = x^3 - 2$ is irreducible over $\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field, b/c $e^{2\pi i/3}\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$.

⑤ $F = \mathbb{Q}$, $f(x) = x^4 - 10x^2 + 1 =$

$$= \prod_{\varepsilon_1, \varepsilon_2 = \pm 1} (x - (\varepsilon_1\sqrt{2} + \varepsilon_2\sqrt{3}))$$

irreducible over $\mathbb{Q}$ (b/c $\pm\sqrt{2} \pm \sqrt{3} \notin \mathbb{Q}$ $\Longrightarrow$ no linear factors, check that there are no quadratic factors, done!)

A root is $\sqrt{2} + \sqrt{3}$. Look at

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) \ni -(\sqrt{2} + \sqrt{3})$$

$$\frac{-1}{\sqrt{2}+\sqrt{3}} = \sqrt{2}-\sqrt{3} \implies \mathbb{Q}(\sqrt{2}+\sqrt{3}) \text{ contains all the roots.}$$

$\therefore \mathbb{Q}(\sqrt{2}+\sqrt{3})$ is the splitting field of f.

Note that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$

($[\subseteq]$ is clear, for $[\supseteq]$, write

$$\sqrt{2} = \frac{1}{2}\left[(\sqrt{2}+\sqrt{3})+(\sqrt{2}-\sqrt{3})\right])$$

$$\begin{array}{c} K = \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3}) \\ |4 \\ \mathbb{Q} = F \end{array}$$

$\mathrm{Aut}(K/F)$ has degree 4. It acts by permutations on both

$\{\sqrt{2},-\sqrt{2}\}$, $\{\sqrt{3},-\sqrt{3}\}$.

and is determined by this perm. representation.

$$\mathrm{Aut}(K/F) \longrightarrow \Sigma_{\{\pm\sqrt{2}\}} \times \Sigma_{\{\pm\sqrt{3}\}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

is an iso (b/c 4 elements + injective).

On the other hand,

$\mathrm{Aut}(K/F) \hookrightarrow S_4$, so we get a non-cyclic transitive subgroup.

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \hookrightarrow S_4.$$

Let us introduce some notation:

$(0,0) \longleftrightarrow \{\sqrt{2} \to \sqrt{2},\ \sqrt{3} \to \sqrt{3}\}$

$(1,0) \longleftrightarrow \{\sqrt{2} \to -\sqrt{2},\ \sqrt{3} \to \sqrt{3}\}$

etc.

Recall: $K \supseteq F$, K splitting field of a separable polynomial f.

$$K = F(\alpha),\ \alpha \text{ a root of } f.$$

$$\# \mathrm{Aut}(K/F) = [K:F]$$

$$\mathrm{Aut}(K/F) \hookrightarrow \Sigma_{\{\text{roots of } f\}}$$

image = transitive subgroup

$\hookrightarrow$ Examples: $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, $\mathbb{F}_{p^m}/\mathbb{F}_p$,

$\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$

<u>Proposition</u>: K field, $H \subseteq \mathrm{Aut}(K)$ subgroup

$$K^H = \{ k \in K \mid h(k) = k, \forall h \in H \}$$
↳ this is a field.

Then: ① If $H_1 \subseteq H$, $K^{H_1} \supseteq K^H$

② If $F_1 \subseteq F_2 \subseteq K$ subfields, then

$$\mathrm{Aut}(K/F_1) \supseteq \mathrm{Aut}(K/F_2)$$

③ $K^{\mathrm{Aut}(K/F)} \supseteq F$, $\mathrm{Aut}(K/K^H) \supseteq H$

<u>Examples</u>: $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$$\left.\begin{tikzcd}[column sep=small]
 & \{(0,0)\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle (0,1) \rangle \arrow[dr, dash] & \langle (1,1) \rangle \arrow[d, dash] & \langle (1,0) \rangle \arrow[dl, dash] \\
 & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} &
\end{tikzcd}\right\} \text{"}H\text{"}$$

$$\left.\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}\right\} \text{"}K^H\text{"}$$

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$$

② Suppose $m | n$, then $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$

Recall $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \langle \mathrm{Fr} \rangle \cong \mathbb{Z}/n\mathbb{Z}$

$$\Rightarrow \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) \cong \underset{\substack{\text{S}\| \\ \langle \mathrm{Fr}^m \rangle}}{m\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{Z}/\left(\tfrac{n}{m}\right)\mathbb{Z}$$

Again, $\exists$ perfect bijection between subfields

$$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^{m'}} \subseteq \mathbb{F}_{p^n}, \quad m | m' | n,$$

and subgroups $m'\mathbb{Z}/n\mathbb{Z}$ via

$$\mathbb{F}_{p^{m'}} \supseteq \mathbb{F}_{p^m} \longleftrightarrow \mathrm{Aut}(\mathbb{F}_{p^{m'}}/\mathbb{F}_{p^m}) \cong m'\mathbb{Z}/n\mathbb{Z}. \checkmark$$

③ $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is NOT a splitting field of x^3-2.

$\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$

$\Rightarrow$ Correspondence between subfields & subgroups is <u>not</u> perfect.

$$\mathbb{Q}(\sqrt[3]{2})^{\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})} = \mathbb{Q}(\sqrt[3]{2})$$

↳ We don't get $\mathbb{Q}$ back!

Def: A finite field extension $K \supseteq F$ is called Galois if

$$\# \mathrm{Aut}(K/F) = [K:F]$$

Notation: $\mathrm{Gal}(K/F) := \mathrm{Aut}(K/F)$

Examples

* $m|n$, $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$
* $\mathbb{Q}(\zeta_n)/\mathbb{Q}$
* $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$

are Galois extensions

* $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is NOT Galois.

Theorem: Let K/F be a splitting field of a polynomial f, then

$$|\mathrm{Aut}(K/F)| \leq [K:F],$$

with equality if f is a separable polynomial, but not if and only if!

Corollary: The splitting field of a separable polynomial is a Galois extension.

Proof: We show by induction on $\deg(f)$ that if

" $F \xrightarrow[\sigma]{\sim} F'$, $f \in F[x]$, $f' = \sigma_*(f) \in F'[x]$,

and $K \supseteq F$ is a splitting field of f,
$K' \supseteq F'$ —"—"—"—"— f',

then $\exists$ at most $[K:F]$ iso φ

$$\begin{array}{ccc} K & \xrightarrow{\varphi} & K' \\ | & & | \\ F & \xrightarrow[\sigma]{\sim} & F' \end{array}$$

and exactly $[K:F]$ if f is separable."

- Clear for $\deg(f) = 1$ $(\Rightarrow K = F \Rightarrow K' = F')$
- Pick an irreducible factor $p(x)$ of $f(x)$, let $p'(x)$ be the corresponding factor of $f'(x)$.

  Pick a root α of $p(x)$ in K and any root β of p' in K'.

$$\begin{array}{ccc} K & & K' \\ | & & | \\ F(\alpha) & \xrightarrow[\sim]{\exists!\, \sigma_\beta} & F'(\beta) \\ | & & | \\ F & \xrightarrow[\sigma]{\sim} & F' \end{array}$$

We have show that $\exists!\ \sigma_\beta : F(\alpha) \to F'(\beta)$ s.t. $\sigma_\beta(\alpha) = \beta$.

$\Rightarrow$ # of σ_β's $\leq$ # β's we can choose in $F' \leq$
$\leq \deg(p') = \deg(p) =$
$= [F(\alpha) : F]$

equality iff $p(x)$ separable

Any
$$\begin{array}{ccc} K & \xrightarrow[\sim]{\tilde{\sigma}} & K' \\ | & & | \\ F & \xrightarrow[\sim]{\sigma} & F' \end{array}$$
restricts to an iso $\sigma_\beta : F(\alpha) \to F'(\beta)$ for some β

(b/c $\tilde{\sigma}(p(\alpha)) = p'(\tilde{\sigma}(\alpha)) \Rightarrow \tilde{\sigma}(\alpha)$ is a root of p')

$\therefore$ If we fix a β, and count $\tilde{\sigma}$ s.t.

$$\begin{array}{ccc} K & \xrightarrow[\sim]{\tilde{\sigma}} & K' \\ | & & | \\ F(\alpha) & \xrightarrow[\sim]{\sigma_\beta} & F'(\beta) \end{array}$$

In this situation, we may apply induction to

$$\frac{f(x)}{(x-\alpha)} \quad \& \quad \frac{f'(x)}{(x-\beta)}$$

to get $\#\tilde{\sigma} \leq [K : F(\alpha)]$ with equality if $f(x)/(x-\alpha)$ separable.

<u>Conclusion 1</u>: $\#\tilde{\sigma} : K \to K$ extending $\sigma : F \to F'$ is

$$\sum_\beta \#\tilde{\sigma} \text{ extending } \sigma_\beta \leq [F(\alpha):F][K:F(\alpha)] = [K:F] \checkmark$$

<u>Conclusion 2</u>: If f is separable, then $\#\beta = [F(\alpha):F]$ and $f(x)/(x-\alpha)$ is separable $\Rightarrow \#\tilde{\sigma}$ for each β is $[K:F(\alpha)]$

$\Rightarrow \#\tilde{\sigma} = [K:F]$ $\square$

Def: A field F is called *perfect* if either:

① $\operatorname{char} F = 0$

② $\operatorname{char} F = p > 0$, and $x \mapsto x^p$ is surjective ($\Rightarrow$ bijective).

Examples: • $F = \mathbb{F}_{p^m}$, $\overline{\mathbb{F}_p}$ are perfect.

∘ $\mathbb{F}_p(t)$ is not perfect (t is not a p^{th} power).

Lemma: Let F be a perfect field and $f \in F[x]$ a non-constant, irreducible polynomial. Then f is separable.

Rmk: We have seen $x^p - t \in \mathbb{F}_p(t)$ is irreducible, but not separable over "$\mathbb{F}_p(t^{1/p})$" $= \mathbb{F}_p(t)/(x^p-t)$, b/c

$$x^p - t = (x - t^{1/p})^p$$

Proof: We know that f is separable iff $\gcd(f', f) = 1$.

If $f' \neq 0$, $\deg(f') < \deg(f)$ and f irred.
$\Longrightarrow \gcd(f', f) = 1$. done!

What if $f' = 0$?

Suppose $f' = 0$, if $f(x) = \sum_{i=0}^{n} a_i x^i$,

$$f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}.$$

$\therefore f' = 0 \Rightarrow \operatorname{ch} F = p > 0$ for some prime p, and each $i > 0$ s.t. $a_i \neq 0$ is divisible by p.

Thus we may write

$$f'(x) = \sum_{1}^{N} b_i x^{pi}$$

Since F is perfect, $b_i = c_i^p$ for some $c_i \in F$

$$\Rightarrow f'(x) = \left(\sum_{1}^{N} c_i x^i \right)^p \Rightarrow$$

$\Rightarrow f'$ is not irreducible $\Rightarrow$

$\Rightarrow f$ is reducible, contradiction!

$\square$

Examples of Galois groups:

* $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$
* $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^2$

* $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$ b/c splitting fld of Φ_n irreducible

* $\mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_{p^n}) \cong m\mathbb{Z}/n\mathbb{Z}$

* $\mathbb{Q}(\omega, \sqrt[3]{2})$ = split. field of x^3-2
(irred. by Eisenstein)
$\Longrightarrow$ separable.

$\mathrm{Gal}(\mathbb{Q}(\omega,\sqrt[3]{2})/\mathbb{Q}) = ?$

Must have 6 elts b/c.

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\omega,\sqrt[3]{2}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\omega) \arrow[dr, dash, "3"'] & & \mathbb{Q}(\sqrt{2}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

On the other hand,

$\mathrm{Gal} \hookrightarrow \Sigma_{\substack{\text{roots}\\ \text{of } x^3-2}} = S_3 \leftarrow$ 6 elts!

$\Longrightarrow \underline{\mathrm{Gal} = S_3}$

* Not Galois: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

$\mathbb{F}_p(t^{1/p})/\mathbb{F}_p(t)$, σ auto, σ permutes the roots of

$x^p - t = (x - t^{1/p})^p \Longrightarrow \sigma = \mathbb{1}$.

$\therefore \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathbb{1}\}$.

§ 4.e The fundamental theorem of Galois theory

November-15-10
10:04 AM

Let G be a group, and L a field.

<u>Def</u>: An L-valued character of G is a homo' of groups

$$\chi : G \longrightarrow L^{\times}.$$

<u>Theorem</u> (Independence of characters)

Let $\chi_1, \dots, \chi_n$ be distinct L-valued characters of G. Then they are linearly independent as functions on G, namely

$$\sum_{i=1}^{n} a_i \chi_i(g) = 0 \quad \forall g \in G \implies a_i = 0 \quad \forall i.$$

<u>Proof</u>: Assume not. Choose a_i, not all zero, s.t. $\sum a_i \chi_i(g) = 0 \quad \forall g \in G$. $(*)$

Choose the relation with the smallest number of non-zero a_i possible.

Changing names, assume $a_1, \dots, a_m \neq 0$ &

$$a_1 \chi_1 + \dots + a_m \chi_m \equiv 0.$$

Choose $g_0 \in G$ s.t. $\chi_1(g_0) \neq \chi_m(g_0)$, recall that χ_i are distinct! Then $\forall g \in G$, $g_0 g \in G$,

$$\implies a_1 \chi_1(g_0 g) + \dots + a_m \chi_m(g_0 g) = 0 \quad \forall g \in G.$$

$\overset{\text{homo'}}{\Longrightarrow}$ $a_1\chi_1(g_0)\chi_1(g)+\dots+a_m\chi_m(g_0)\chi_m(g)=0$

On the other hand $\chi_m(g_0)\cdot 0=0 \Longrightarrow$

$$a_1\chi_m(g_0)\chi_1(g)+\dots+a_m\chi_m(g_0)\chi_m(g)=0$$

Substracting, we get

$$a_1\big(\chi_1(g_0)-\chi_m(g_0)\big)\chi_1(g)+\dots+$$
$$+\,a_{m-1}\big(\chi_{m-1}(g_0)-\chi_m(g_0)\big)\chi_{m-1}(g)+0=0$$

As $\chi_1(g_0)\neq\chi_m(g_0)$, this is a non-trivial linear combination with <u>fewer</u> non-zero elements. Contradiction to minimality of (*)

$\square$

<u>Corollary</u>: If $\sigma_1,\dots,\sigma_n$ are distinct field embeddings $K\to L$, then they are lin. indep. over L.

Recall, a field embedding $\sigma: K\to L$ is just a field homo'.

<u>Proof</u>: Dependence $\Longrightarrow$ Dependence of

$\sigma_i|_{K^\times}: K^\times \longrightarrow L^\times$, characters!

Still distinct!

$\square$

Theorem: Let G be a finite group of automorphisms of a field K.

If $F = K^G = \{ k \in K \mid \forall g \in G,\ g(k) = k \}$,

then $[K : F] = \# G$.

Proof: Let $G = \{\sigma_1, \dots, \sigma_n\}$.

I. Suppose $n > [K:F]$, we will show that $\{\sigma_1, \dots, \sigma_n\}$ are lin. dep. contradicting the corollary above.

Let $m = [K:F]$ and let $\{\omega_1, \dots, \omega_m\}$ be a basis for K/F. Consider the following system of m lin. equations in n variables

$$\begin{cases} \sigma_1(\omega_1) x_1 + \dots + \sigma_n(\omega_1) x_n = 0 \\ \dots \\ \sigma_1(\omega_m) x_1 + \dots + \sigma_n(\omega_m) x_n = 0 \end{cases}$$

As $m < n$, $\exists$ non-trivial solution, say $(a_1, \dots, a_n) \in K^n$ s.t. $\forall j \le m$,

$$\sum_{i=1}^{n} \sigma_i(\omega_j) a_i = 0$$

$\therefore$ The F-linear function $\sum_i \sigma_i(\cdot) a_i$ vanishes on every basis vector $\omega_j \Longrightarrow$
$\Longrightarrow \sum_i \sigma_i(x) a_i = 0, \ \forall x \in K$

$\Longrightarrow \{\sigma_i\}$ are lin. dep. Contradiction!

II. Suppose $n < [K:F]$ ($[K:F]$ need not be even finite!) Let $\{\alpha_1, \dots, \alpha_{n+1}\}$ be lin. indep. in K/F. Consider the following system of n lin. eq. in $(n+1)$ unknowns

$$\begin{cases} \sigma_1(\alpha_1)x_1 + \dots + \sigma_1(\alpha_{n+1})x_{n+1} = 0 \\ \sigma_n(\alpha_1)x_1 + \dots + \sigma_n(\alpha_{n+1})x_{n+1} = 0 \end{cases}$$

$\Longrightarrow \exists$ non-trivial sol'n, say $(\beta_1, \dots, \beta_{n+1}) \in K^{n+1}$.

Now, choose a non-trivial solution with the least number of non-zero β_i's. WLOG, assume that $\beta_1, \dots, \beta_r \neq 0$ and $\beta_{r+1}, \dots, \beta_{n+1} = 0$. Further, dividing by $\beta_r \neq 0$, we may assume that $\beta_r = 1$.

Moreover, at least one $\beta_i \notin F$, because otherwise $\beta_1\alpha_1 + \dots + \beta_r\alpha_r = 0$ shows linear dep. of $\{\alpha_i\}$ in K/F, contradiction. Thus, by reindexing, we can assume $\beta_1 \notin F$. So, we get

$$\begin{cases} \sigma_1(\alpha_1)\beta_1 + \dots + \sigma_1(\alpha_{r-1})\beta_{r-1} + \sigma_1(\alpha_r) = 0 \\ \dots \\ \sigma_n(\alpha_1)\beta_1 + \dots + \sigma_n(\alpha_{r-1})\beta_{r-1} + \sigma_n(\alpha_r) = 0 \end{cases} \quad (1)$$

Applying some $\sigma \in G$ to (1), we have

$$\begin{cases} \sigma(\sigma_1(\alpha_1)\beta_1) + \dots + \sigma(\sigma_1(\alpha_{r-1})\beta_{r-1}) + \sigma(\sigma_1(\alpha_r)) = 0 \\ \dots \\ \sigma(\sigma_n(\alpha_1)\beta_1) + \dots + \sigma(\sigma_n(\alpha_{r-1})\beta_{r-1}) + \sigma(\sigma_n(\alpha_r)) = 0 \end{cases} \quad (1_\sigma)$$

As $\sigma(\{\sigma_1, \dots, \sigma_n\}) = \{\sigma_1, \dots, \sigma_n\}$, (1_σ) is in fact equal to (by reordering rows),

$$\begin{cases} \sigma_1(\alpha_1)\sigma(\beta_1) + \dots + \sigma_1(\alpha_r) = 0 \\ \sigma_n(\alpha_1)\sigma(\beta_1) + \dots + \sigma_n(\alpha_r) = 0 \end{cases} \quad (2_\sigma)$$

As $\beta_1 \notin F$, $\exists \sigma_0 \in G$ s.t. $\sigma_0(\beta_1) \notin \{\beta_1, \dots, \beta_r\}$, so then, substracting $(1) - (2_\sigma)$ we get

$$\begin{cases} \sigma_1(\alpha_1)\left[\beta_1 - \sigma_0(\beta_1)\right] + \dots + \sigma_1(\alpha_{r-1})\left[\beta_r - \sigma_0(\beta_r)\right] = 0 \\ \quad \vdots \\ \sigma_n(\alpha_1)\left[\beta_1 - \sigma_0(\beta_1)\right] + \dots + \sigma_n(\alpha_{r-1})\left[\beta_r - \sigma_0(\beta_r)\right] = 0 \end{cases}$$

$\therefore \{(\beta_i - \sigma_0(\beta_i))\}_{i=1}^{r-1}$ is a shorter non-trivial (b/c $\beta_1 - \sigma_0(\beta_1) \neq 0$) solution.

Contradiction!

$\square$

<u>Corollary</u>: Let K/F be a finite extension, then

$$|\mathrm{Aut}(K/F)| \leq [K:F]$$

with equality iff

$$F = K^{\mathrm{Aut}(K/F)}$$

<u>Proof</u>: Let $G = \mathrm{Aut}(K/F)$. As K/F is a finite extension,

$$K = F(\alpha_1, \dots, \alpha_t)$$

Then, the action of G on K is determined by its action on $\{\alpha_1, \dots, \alpha_t\}$. If f_i is the minimal poly of α_i over F, then

$$G \hookrightarrow \Sigma_{\substack{\text{roots}\\ \text{of } f_1}} \times \dots \times \Sigma_{\substack{\text{roots}\\ \text{of } f_t}}$$

finite group.

$\therefore G$ is finite.

We have $F \subseteq K^G \subseteq K$, and

$$[K:F] = [K:K^G][K^G:F] \overset{\text{Thm}}{=} |G| \cdot [K^G:F] \geq |G|$$

with equality iff $[K^G:F] = 1$, i.e. $K^G = F$

$\square$

Remark: If $[K:F] = |Aut(K/F)|$, we said that the extension K/F was Galois. Thus, we can reformulate the statement of the last corollary as

$$K/F \text{ is Galois iff } F = K^{Aut(K/F)}$$

Corollary: Let $G < Aut(K/F)$ be a finite subgroup, then $Aut(K/K^G) = G$ and K/K^G is Galois.

Proof: Clearly $G \subseteq Aut(K/K^G)$, so by theorem,

$$|G| \overset{\text{Thm}}{=} [K:K^G] \overset{\text{Cor}}{\geq} |Aut(K/K^G)| \geq |G|$$

$\therefore\ |G| = |\mathrm{Aut}(K/K^G)|$, so by corollary, K/K^G is Galois.

$\square$

<u>Corollary</u>: If $G_1 \neq G_2$ are finite subgroups of $\mathrm{Aut}(K/F)$, then

$$K^{G_1} \neq K^{G_2}$$

<u>Proof</u>: By previous corollary,

$$\mathrm{Aut}(K/K^{G_1}) = G_1 \neq G_2 = \mathrm{Aut}(K/K^{G_2})$$

$\square$

We will now prove one last way of characterizing a Galois extension K/F.

<u>Theorem</u>: If K/F is Galois, then K is the splitting field of a separable poly $f \in F[x]$.

<u>Proof</u>: Let $G = \mathrm{Gal}(K/F) = \{1 = \sigma_1, \sigma_2, \dots, \sigma_n\}$

Let $\alpha \in K$ and consider the "conjugates" of α

$$\{\alpha = \sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_n(\alpha)\}$$

This set need not contain n distinct elements, but we can pick

$$\{\alpha = \alpha_1, \dots, \alpha_t\} \text{ distinct conjugates.}$$

Consider a poly $f(x) = \sum a_i x^i$ defined by

$$f(x) = \prod_{i=1}^{t} (x - \alpha_i) \in K[x]$$

Then $\forall \sigma \in G$, $\sum \sigma(a_i) x^i = \prod_{i=1}^{t} (x - \sigma(\alpha_i)) =$

b/c $\sigma(\{\alpha_i\}_i) = \{\alpha_i\}_i$ $\quad = \prod_{i=1}^{t} (x - \alpha_i)$

$\therefore \sum a_i x^i = \sum \sigma(a_i) x^i \quad \forall \sigma \in G \implies$

$\implies a_i \in K^G = F$ (b/c K/F Galois)

Hence, any $\alpha \in K$ satisfies a separable poly $f_\alpha \in F[x]$, s.t. all roots of f_α are in K.

Since K/F is a finite extension, $K = F(\beta_1, \dots, \beta_m)$
$\implies$ The poly $(f_{\beta_1} \cdot \ldots \cdot f_{\beta_m})(x) \in F[x]$ splits in K.

Now, delete all f_{β_i} that appear twice (if any) to obtain a separable polynomial that splits over K, i.e. K is its splitting field.

$\square$

Remark : The poly $f_\alpha \in F[x]$ is in fact **irreducible** over F. In fact, if $g \mid f_\alpha$, $g \in F[x]$, g non-constant, then some α_i solves g.

$$g(\alpha_i) = 0 \implies g(\sigma(\alpha_i)) = \sigma(g(\alpha_i)) = \sigma(0) = 0 \quad \forall g \in G$$

$\therefore$ As all roots of f_α are of the form $\sigma(\alpha_i)$ for some $\sigma \in G$, the roots of g and f_α are the same $\implies g = f$ up to a scaling factor.

Example : $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $(x^2-2)(x^2-3)$, separable.

$\implies \mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}$ is Galois.

By remark, we can easily find the min. poly of $\alpha = (\sqrt{2} + \sqrt{3}) \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$:

Take $f(x) = \prod_{i=1}^{4} (x - \alpha_i) =$

$$= (x - (\sqrt{2} + \sqrt{3}))(x - (\sqrt{2} - \sqrt{3}))(x + (\sqrt{2} - \sqrt{3}))(x + (\sqrt{2} + \sqrt{3}))$$
$$= (x^2 - 2)(x^2 - 3)$$

$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
|
$\mathbb{Q}(\sqrt{2})$
|
$\mathbb{Q}$

$H = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}(\sqrt{2})) = \left\{ 1, \begin{bmatrix} \sqrt{2} \to \sqrt{2} \\ \sqrt{3} \to -\sqrt{3} \end{bmatrix} \right\}$

$\implies$ min. poly. of $(\sqrt{2} + \sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$ is $x^2 - 2\sqrt{2}\,x + 1 =$

$$= (x - (\sqrt{2} + \sqrt{3}))(x - (\sqrt{2} - \sqrt{3})) \checkmark$$

Def: An extension K/F is said to be **normal** if every poly in $F[x]$ with a root in K splits over K.

Def: An extension K/F is called **separable** if every $\alpha \in K$ is a root of a separable poly in $F[x]$.

Theorem: (Portmanteau theorem for Galois extensions.)

Let K/F be a finite extension. TFAE

1. K/F is Galois, i.e. $[K:F] = |\mathrm{Aut}(K/F)|$ (equivalently $[K:F] \geq |\mathrm{Aut}(K/F)|$ because "$\leq$" is always true).
2. $F = K^{\mathrm{Aut}(K/F)}$
3. K is the splitting field of a separable poly $f \in F[x]$.
4. The extension K/F is separable and normal.

Proof: We have shown 1 – 3 already. The equivalence of 4 is left as an exercise.

$\square$

Main theorem of Galois theory

November-22-10
10:08 AM

Theorem: Let K/F be a Galois extension, $G = \mathrm{Aut}(K/F)$. Then there is a bijection

$$\left\{\begin{array}{c}\text{Subfields } E \text{ of } K \\ F \subseteq E\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{Subgroups} \\ \text{of } G\end{array}\right\}$$

$$E \longmapsto \mathrm{Aut}(K/E)$$

$$K^H \longleftarrow\!\shortmid\; H$$

In particular these two operations are mutual inverses and

1. $H_1 \subseteq H_2 \implies K^{H_1} \supseteq K^{H_2}$
   $K_1 \subseteq K_2 \implies \mathrm{Aut}(K/K_1) \supseteq \mathrm{Aut}(K/K_2)$

2. $[K : K^H] = |H|$ & $[K^H : F] = [G : H]$

3. K/E is Galois and if $E = K^H$, $\mathrm{Aut}(K/E) = H$

4. $K^{H_1} \cap K^{H_2} = K^{\langle H_1, H_2 \rangle}$
   $K^{H_1} K^{H_2} = K^{H_1 \cap H_2}$

5. $E = K^H$ is Galois over F iff $H \trianglelefteq G$ and in that case

$$\mathrm{Aut}(E/F) \cong G/H$$

<u>Proof</u>: G is finite ($|G| = [K:F]$) and we have already shown that for $H \subseteq Aut(K/F)$, finite, the extension K/K^H is Galois, $Aut(K/K^H) = H$.

Thus, $H \longmapsto K^H$ is injective ✓

Since K is the splitting field of a separable poly $f \in F[x] \subseteq E[x]$, K/E is also Galois
$\Longrightarrow E = K^{Aut(K/E)}$

As $H = Aut(K/E) < Aut(K/F) = G$, $H \mapsto K^H$ is also surjective. ✓

Also, the identity $Aut(K/K^H) = H$ shows that $E \to Aut(K/E)$ is the inverse of $H \to K^H$.

Furthermore, K/K^H Galois $\Longrightarrow$
$\Longrightarrow [K:K^H] = |Aut(K/K^H)| = |H|$, and as $F = K^G$,

$$[K^H : F] = \frac{[K:F]}{[K:K^H]} = \frac{|G|}{|H|} = [G:H]$$

which finishes the proof of ① – ③. ✓

④ follows directly from the fact that we have an order reversing bijection between two posets. ✓

To prove ⑤, we need a little more work however.

Consider all field homo's $E \to K$ that fix F. We know that if $\tau \in G = Gal(K/F)$, then $\tau \in Hom_F(E,K)$

$$\begin{tikzcd} K \arrow[r, "\tau"] & K \\ E \arrow[u, dash] \arrow[r, "\tau|_E"] & K \arrow[u, phantom, "\cup" rotate=90] \\ F \arrow[u, dash] \arrow[r, "id"] & F \arrow[u, phantom, "\cup" rotate=90] \end{tikzcd}$$

Thus, we get a map $Aut(K/F) \to Hom_F(E,F)$.

$\hookrightarrow$ This map is surjective

As K/F is Galois, K is the splitting field of a separable poly $f \in F[x] \subseteq E[x]$, then

$$\begin{tikzcd} \text{splitting field of } f = K \arrow[r, "\exists\tau"] & K = \text{splitting field of } \sigma_* f(x) = f(x) \\ E \arrow[u, dash] \arrow[r, "\sigma"] & \sigma(E) \arrow[u, dash] \\ F \arrow[u, dash] \arrow[r, "id"] & F \arrow[u, dash] \end{tikzcd}$$

Hence, by theorem, $\exists \tau : K \to K$, $\tau|_E = \sigma$

But, given $\tau_1, \tau_2 \in Aut(K/F)$, we have

$$\tau_1|_E = \tau_2|_E \iff \tau_2^{-1}\tau_1|_E = id_E \iff$$
$$\iff \tau_2^{-1}\tau_1 \in Aut(K/E) \iff$$
$$\iff \tau_1 Aut(K/E) = \tau_2 Aut(K/E).$$

$\therefore$ We have a bijection between two <u>sets</u>

$$Aut(K/F)/Aut(K/E) \longleftrightarrow Hom_F(E,K)$$

Note that $Aut(E/F) \subseteq Hom_F(E,K)$, and

$$\left|Aut(E/F)\right| \leq [E:F] = \frac{|Aut(K/F)|}{|Aut(K/E)|} = \left|Hom_F(E,K)\right|$$

↑ b/c bijection

$\therefore$ We get equality $|Aut(E/F)| = |Hom_F(E,K)|$ iff $|Aut(E/F)| \overset{?}{=} [E:F]$, i.e. iff E/F is Galois.

E/F is Galois $\iff Aut(E/F) = Hom_F(E,K) \iff$

$\iff$ Every embedding of E/F into K/F is an auto. $\iff \forall \sigma \in Gal(E/F), \sigma(E) = E$

$\overset{!}{\iff} \forall \sigma \in Gal(E/F)$,

$$\sigma^{-1} H \sigma = Aut(K/\sigma(E)) = Aut(K/E) = H$$

$\iff H \triangleleft Gal(K/F)$.

Therefore if (and only if) $H \triangleleft Gal(K/F)$

$$Aut(K/F)/Aut(K/E) \cong Aut(E/F) \text{ as groups.}$$

$\square$

<u>Corollary</u>: If $F \subseteq K \subseteq \bar{K}$, $\bar{K}/F$ is Galois, then $\exists$ only finitely many subfields $F \subseteq E \subseteq K$.

<u>Proof</u>: By theorem, every such subfield corresponds to a subgroup of $Gal(\bar{K}/F)$, a finite group. Every finite group has only finitely many subgroups. $\square$

<u>Remark</u>: Examples show that if K/F is a finite extension that is NOT Galois, then there can be an infinite number of subfields.

§ 4.f Examples

November-24-10
10:11 AM

① $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2 = G$

$$\begin{tikzcd}[column sep=small]
 & (\mathbb{Z}/2\mathbb{Z})^2 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle(1,0)\rangle \arrow[dr, dash] & \langle(1,1)\rangle \arrow[d, dash] & \langle(0,1)\rangle \arrow[dl, dash] \\
 & \langle(0,0)\rangle &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & \mathbb{Q} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) &
\end{tikzcd}$$

Every $E/\mathbb{Q}$ is Galois b/c G is abelian.
(Check: $\mathbb{Q}(\sqrt{d})$ = split. of x^2-d if d is not a square).

② $m \mid n$, $\quad F := \mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} =: K$

$\mathrm{Gal}(K/F) \cong m\mathbb{Z}/n\mathbb{Z}$ ← generated by $\mathrm{Fr}^{\circ m}$

Galois correspondence is what we have seen if $m \mid m' \mid n$,

$$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^{m'}} \subseteq \mathbb{F}_{p^n} \longleftrightarrow n\mathbb{Z} \subseteq m'\mathbb{Z} \subseteq m\mathbb{Z}$$

③ Cyclotomic fields: $n \geq 1$, integer, $\zeta_n = e^{\frac{2\pi i}{n}}$

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

$\forall a \in \mathbb{Z}/n\mathbb{Z}$, auto' σ_a is determined by

$$\sigma_a(\zeta_n) = \zeta_n^a$$

Again, every subfield of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois over $\mathbb{Q}$, but the description of the subfields is more involved.

A. Take $n=7$: $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^\times$

cyclic group of order 6

$\Rightarrow \exists$ 2 non-trivial subgroups of $(\mathbb{Z}/7\mathbb{Z})^\times$.

Let $H < (\mathbb{Z}_7)^\times$, define

$$\mathbb{Q}(\zeta_7) \xrightarrow{\pi} \mathbb{Q}(\zeta_7)^H$$

$$t \longmapsto \frac{1}{|H|} \sum_{h \in H} h(t)$$

linear map of $\mathbb{Q}$-v.sp., identity on $\mathbb{Q}(\zeta_7)^H$
$\Rightarrow \pi$ is a (surjective) projection onto $\mathbb{Q}(\zeta_7)^H$.

If $\{t_1, t_2, \dots\}$ are a basis for $\mathbb{Q}(\zeta_7)/\mathbb{Q}$, then $\mathbb{Q}(\zeta_7)^H = \mathbb{Q}(\pi(t_1), \dots)$

b/c $\mathbb{Q}(\zeta_7) = \mathbb{Q}(\underbrace{\{\zeta_7^a : (a,7)=1\}}_{\text{basis for } \mathbb{Q}(\zeta_7)/\mathbb{Q}})$

splitting field of $\Phi_7(x)$

$$\mathbb{Q}(\zeta_7) \supseteq \sum_{(a,7)=1} \mathbb{Q}\cdot\zeta_7^a \supseteq \mathbb{Q}$$

dim $\leq \varphi(7)$

dim $= \varphi(7)$

Also, we know $\mathbb{Q}(\zeta_7) \cong \mathbb{Q}[x]/(\Phi_7(x))$

and so, spanned by $1, x, \dots, x^6$, which works b/c $7 =$ prime.

↳ This is still true for a general n, but we need an extra argument.

B. Let $N \geq 1$, $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ is Galois,

$$G = \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times \text{ with}$$
$$a \longmapsto \sigma_a(\zeta_N) = \zeta_N^a$$

Any $H < G$ is normal and

$\mathbb{Q}(\zeta_N)/\mathbb{Q}$ is Galois with Galois gp $(\mathbb{Z}/N\mathbb{Z})^\times/H$

Defined an averaging operator $\mathbb{Q}(\zeta_N) \to \mathbb{Q}(\zeta_N)^H$

$$t \longmapsto \frac{1}{|H|}\sum_{h\in H} h(t)$$

Then $\mathbb{Q}(\zeta_N) \supseteq \bigoplus_{(a,N)=1} \mathbb{Q} \cdot \zeta_N^a$

If we show that $\{\zeta_N^a : (a,N)=1\}$ is lin indep. over $\mathbb{Q}$, then the sum is indeed direct and

$$\mathbb{Q}(\zeta_N) = \bigoplus_{(a,N)=1} \mathbb{Q} \cdot \zeta_N^a$$

Assume N is prime, write

$$\mathbb{Q}(\zeta_N) = \mathbb{Q}[x]/(\Phi_N(x)), \quad \Phi_N(x) = \frac{x^N - 1}{x-1} = 1 + x + \dots + x^{N-1}$$

$\Longrightarrow \{\bar{1}, \bar{x}, \dots, \overline{x^{N-2}}\}$ are lin. indep. $\Longrightarrow$

$\Longrightarrow \{\bar{x}, \overline{x^2}, \dots, \overline{x^{N-1}}\}$ are lin. indep. $\Longrightarrow$

$\Longrightarrow \{\zeta, \zeta^2, \dots, \zeta^{N-1}\}$ indep. over $\mathbb{Q}$.

$\therefore \mathbb{Q}(\zeta_N)^H = \mathbb{Q}(\{\pi(\zeta_N^a) : (a,N)=1\}) \overset{!}{=}$ by remark on the next page.

$= \mathbb{Q}(\pi(\zeta_N))$

G abelian.

Note: $\pi(\zeta_N^a) = \pi(\sigma_a(\zeta_N)) = \sigma_a(\pi(\zeta_N))$

The field $\mathbb{Q}(\pi(\zeta_N))$ is Galois over $\mathbb{Q}$, and so, by remark,

$$\sigma_a(\pi(\zeta_N)) \in \mathbb{Q}(\pi(\zeta_N)) \quad \forall \sigma_a \in G.$$

$$\mathbb{Q}(\zeta_N)^H = \mathbb{Q}(\pi_H(\zeta_N)), \quad \pi_H(t) = \frac{1}{|H|}\sum_{h\in H} h(t)$$

<u>General remark</u>: K/F Galois, $K \subseteq L$, then any $\sigma \in \mathrm{Aut}(L/F)$ satisfies $\sigma(K) \subseteq K$.

Indeed, $K =$ split. field of a sep. poly $f \in F[x]$.
$= F(\alpha_1, \dots, \alpha_N)$ roots of f

$$\sigma(K) = F(\sigma(\alpha_1), \dots, \sigma(\alpha_N)) = F(\alpha_1, \dots, \alpha_N)$$

If $N = 7$, $(\mathbb{Z}/7\mathbb{Z})^\times = \{3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1\} = \langle 3 \rangle$

Cyclic subgroup of order 3 is $\langle 3^2 \rangle = \{2, 4, 8 = 1\}$
— " — " — " — 2 is $\langle 3^3 \rangle = \{\pm 1\}$.

Let $\omega = \zeta_7 = e^{\frac{2\pi i}{7}}$

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\omega) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\omega)^H \arrow[dr, dash, "2"] & & \mathbb{Q}(\omega)^J \arrow[dl, dash, "3"'] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & (\mathbb{Z}/7\mathbb{Z})^\times \arrow[dl, dash] \arrow[dr, dash] & \\
H = \langle 3^2 \rangle \arrow[dr, dash] & & J = \langle 3^3 \rangle \arrow[dl, dash] \\
 & \{1\} &
\end{tikzcd}$$

$\mathbb{Q}(\omega)^H = \mathbb{Q}(\omega + \omega^2 + \omega^4)$, $\mathrm{Gal} = (\mathbb{Z}/7\mathbb{Z})^\times / \{1, 2, 4\}$

$\mathbb{Q}(\omega)^J = \mathbb{Q}(\omega + \omega^{-1})$, Galois $\cong (\mathbb{Z}/7\mathbb{Z})^\times / \{\pm 1\}$

$$\mathbb{Q}(\omega)^H = \mathbb{Q}[x]/(f(x)), \quad f = \text{min. poly of } \omega + \omega^2 + \omega^4$$

Know: $f(x) = \prod (x - \alpha)$ $\quad$ α conjugate of $\omega+\omega^2+\omega^4$

$$\sigma_3(\omega+\omega^2+\omega^4) = \omega^3+\omega^6+\omega^{12} = \omega^3+\omega^5+\omega^6$$

$$= \left(x - (\omega+\omega^2+\omega^4)\right)\left(x - (\omega^3+\omega^5+\omega^6)\right) =$$

$$= x^2 - \underbrace{(\omega+\dots+\omega^6)}_{=-1} x + (\omega+\omega^2+\omega^4)(\omega^3+\omega^5+\omega^6)$$

b/c $1+\omega+\dots+\omega^6 = 0.$

$$= x^2 + x + 2$$

$$\therefore \mathbb{Q}(\zeta_7)^H = \mathbb{Q}(\sqrt{-7})$$

---

(4) K = split field of $x^p - \ell$ over $\mathbb{Q}$, p, ℓ primes

By Eisenstein, $x^p - \ell$ is irreducible.

$$K = \mathbb{Q}\left(\{\zeta^a \cdot \sqrt[p]{\ell} : \zeta = \zeta_p, a = 1, \dots, p-1\}\right) =$$

$$= \mathbb{Q}(\zeta_p, \sqrt[p]{\ell})$$

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\zeta_p, \sqrt[p]{\ell}) \arrow[dl, no head] \arrow[dr, no head] & \\
\mathbb{Q}(\zeta_p) \arrow[dr, no head, "p-1"] & & \mathbb{Q}(\sqrt[p]{\ell}) \arrow[dl, no head, "p"'] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$$\therefore [\mathbb{Q}(\zeta_p, \sqrt[p]{\ell}) : \mathbb{Q}] = p(p-1)$$

Any $\sigma \in G = \mathrm{Gal}(K/\mathbb{Q})$ is determined by

$$\begin{cases} \sigma(\zeta_p) = \zeta_p^{a}, & 1 \leq a \leq p-1 \\ \sigma(\sqrt[p]{\ell}) = \zeta_p^{b}\sqrt[p]{\ell}, & 0 \leq b \leq p-1 \end{cases}$$

$\rightarrow$ # of possibilities $= p(p-1) = |G|$

$\Longrightarrow$ any such (a,b) appears for some $\sigma \in G$.

Notation: $\sigma = \sigma_{a,b}$.

Compute: $\sigma_{a_1,b_1} \circ \sigma_{a_2,b_2}$

* $\sigma_{a_1,b_1}(\sigma_{a_2,b_2}(\zeta_p)) = \zeta_p^{a_1a_2}$

* $\sigma_{a_1,b_1}(\sigma_{a_2,b_2}(\sqrt[p]{\ell})) = \zeta_p^{a_1b_2+b_1}\sqrt[p]{\ell}$

$\therefore \sigma_{a_1,a_2} \circ \sigma_{a_2,b_2} = \sigma_{a_1a_2,\, a_1b_2+b_1}$

Note that $\begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2+b_1 \\ 0 & 1 \end{pmatrix}$

$$\Longrightarrow G \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/p\mathbb{Z}) \right\}$$

<u>Proposition</u>: $f(x) \in \mathbb{Q}[x]$ an irreducible poly of degree 5 with exactly 3 real roots.

$K =$ split. field of $f \subseteq \mathbb{C}$. Then

$$G = \mathrm{Gal}(K/\mathbb{Q}) \cong S_5$$

<u>Proof</u>: Let α be a root of f, then

$$\begin{array}{c} K \\ | \\ \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q} \end{array} \qquad \begin{array}{l} \& \ [\mathbb{Q}(\alpha):\mathbb{Q}] = 5 \implies \\ \\ \implies 5 \mid \# S_5 . \end{array}$$

On the other hand, $G \hookrightarrow \Sigma_{\{\text{roots of } f\}} \cong S_5$

Complex conjugation acts on K (b/c $K/\mathbb{Q}$ Galois, $K \subseteq \mathbb{C}$)

$$\begin{tikzcd} \mathbb{C} \arrow[r, "c.c."] & \mathbb{C} \\ K \arrow[u, dash] \arrow[r] & K \arrow[u, dash] \end{tikzcd}$$

But $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_5)$ roots of f, 3 of them are real. Therefore c.c. is a transposition of the two non-real roots.

Since G contains an elt. of order 5, wlog, $(12345) \in G$, and $(ij) \in G$.

Conjugate (ij) by (12345) to get $(i+1, j+1) \in G$

$\therefore\ (i+a,\ j+a) \in G, \quad 0 \le a \le 4.$
distinct transpositions.

$\Rightarrow$ G contains 5 elts of order 2.

$\Rightarrow \{1, (i,j), (i+a, j+a), (i,j)(i+a, j+a)\}$ has order 4 if a is chosen appropriately.

Also, $(i,j)(j = i+a,\ 2j-i) = \underbrace{(i, j, 2j-i)}_{\text{order } 3} \in G$

$\therefore\ |G|$ is divisible by $4,3,5 \Rightarrow 60 \mid |G|$

$\Rightarrow$ Either $G = S_5$, or $|G| = 60$ and $G \triangleleft S_5$

As in S_5, σ is conj. to $\tau \Leftrightarrow$ they have the same cycle type, G must contain all these cycle types:

	#
(1)	1
(12)	10
(123)	20
(12)(34)	15
(12345)	24
(123)(45)	20
(1234)	30

(first five rows) $= 70 > 60 \Rightarrow |G| = 120$ $\square$

Alternatively, $A_5 \triangleleft S_5$ is simple
$\#(G \cap A_5) > 1$ b/c
$120 = \# S_5 \ge \# G \cdot A_5 = \dfrac{\# G\ \# A_5}{\# G \cap A_5}$

Now $G \triangleleft S_5 \Rightarrow G \cap A_5 \triangleleft A_5 \overset{\text{simple}}{\Rightarrow} G \supseteq A_5$

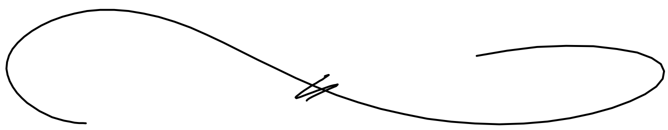
Finally, $\underset{\text{odd}}{(12)} \in G \Rightarrow G = S_5$.

$\square$

Example : $f(x) = x^5 - 6x + 3$

$f(-2) = -17$, $f(0) = 3$, $f(1) = -2$, $f(2) = 23$

$f'(x) = 5x^4 - 6$ has 2 real roots



§ 4.g Radical extensions and some further topics

November-29-10
9:45 AM

<u>Def</u>: A finite extension K/F is called radical if $\exists \underbrace{\tilde{K} \supseteq K \supseteq F}_{\text{finite}}$ and

$\tilde{K} = F(\alpha_1, \dots, \alpha_n)$ s.t. $\forall i$, $\exists n_i$ s.t.

$$\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$$

($\tilde{K}$ is obtained from K by repeatedly taking roots!)

<u>Def</u>: We say that a poly $f \in F[x]$ can be solved in radicals if it has a splitting field K s.t. K/F is a radical extension.

<u>Theorem</u> (Galois)

A separable polynomial $f(x) \in F[x]$ can be solved in radicals iff

$Gal(K/F)$ is a solvable group.

<u>Corollary</u>: The general equation of degree 5 cannot be solved in radicals

<u>Proof</u>: $\exists$ such poly. with Galois gp. S_5, which is not solvable.

- A_5 is a simple group (true for any $A_n, n \geq 5$)

$\hookrightarrow$ Conjugacy classes in A_5 are

Conj. classes	#
(1)	1
(123)	20
$(12)(34)$	15
(12345)	12
(12354)	12

$(\circledast)$

Since any normal subgroup is a disjoint union of conjugacy classes, and the only partial sums in $\circledast$ dividing 60 are 1 & 60, any normal subgroup is trivial.

- Hence A_5 not solvable $\Rightarrow S_5$ not solv.

$\square$

<u>Corollary</u>: On the other hand, for a poly of degree < 5,

$$\text{Gal. gp. } G \hookrightarrow S_n \quad , n = \deg(f).$$

$$\Rightarrow \# G < 60 \overset{\text{Exercise}}{\Longrightarrow} G \text{ is solvable} \Rightarrow$$

$\rightarrow$ can solve f in radicals.

$\square$

Some general results from Galois theory

November-29-10
10:01 AM

I. K_1/F, K_2/F are Galois extensions, then $(K_1K_2)/F$ & $(K_1 \cap K_2)/F$ are Galois!

↳ For $(K_1K_2)/F$ use splitting fields

→ For $(K_1 \cap K_2)/F$ use finite, normal, sep. extension characterization.

II. One can show

$$\mathrm{Gal}(K_1K_2/F) \hookrightarrow \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$$

$$\sigma \longmapsto \left(\sigma|_{K_1}, \sigma|_{K_2}\right)$$

$$\text{Image} = \left\{ (\alpha, \beta) : \alpha|_{K_1 \cap K_2} = \beta|_{K_1 \cap K_2} \right\}$$

III. K/F Galois, F_1/F any extension, then

KF_1/F_1 is Galois (by split. field arg.), and

$$\begin{tikzcd}
 & KF_1 \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & F_1 \arrow[dl, dash] \\
 & K \cap F_1 \arrow[d, dash] & \\
 & F &
\end{tikzcd}$$

$$\mathrm{Gal}(KF_1/F_1) \cong \mathrm{Gal}(K/K \cap F_1)$$

$$\sigma \longmapsto \sigma|_K$$

(Hard part is to prove that the map is surjective)!

IV. The discriminant.

F field of char. $\neq 2$.

$f(x)$ monic, irred. sep. poly $\in F[x]$. of degree n.

K splitting field, $G = \mathrm{Gal}(K/F)$.

$G \hookrightarrow S_n$ (image = trans. subgroup)

$\{\alpha_1, \dots, \alpha_n\}$ roots of f, embedding is through action on roots.

$$\delta := \prod_{i<j} (\alpha_i - \alpha_j)$$

If $\sigma \in G \subseteq S_n$, then $\sigma(\delta) = \mathrm{sgn}(\sigma) \cdot \delta$

So, $G \subseteq A_5 \iff \sigma(\delta) = \delta \;\; \forall \sigma \in G$.
At any rate $\sigma(\delta^2) = \sigma(\delta)^2 = \delta^2 \;\; \forall \sigma \in G$

$$\implies \delta^2 \in F.$$

Def: We define the discriminant of $f \in F[x]$.

$$\mathcal{D}(f) := \delta^2$$

To say G fixes δ is to say $\sqrt{\mathcal{D}(f)} \in F$.

Conclusion: $G \subseteq A_5 \iff \mathcal{D}(f)$ is a square in F.

$D(f)$, being a symm. function in the roots of f is thus a poly. in the coeff of f.

Example: $x^2 + bx + c = f(x)$

$$D(f) = (\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 =$$

$$= \underline{b^2 - 4c}$$

Example: If $\mathrm{char}(F) \neq 3$,

$$f(x) = x^3 + \alpha x^2 + \beta x + \gamma$$

Put $x = y - \alpha/3 \rightsquigarrow y^3 + Ay + B = g(y)$
and

$$D(g) = -4A^3 - 27B^2$$

(by laborious calculation ....)

Example: $f(x) = x^3 - x + 1$ irreducible (by Rational Roots thm).

$D(f) = -23 \Rightarrow$ not a square

$\Rightarrow G \not\subseteq A_3$, but is transitive $\Rightarrow G = S_3$ ✓

Example: $x^3 - 21x - 7$ irred. by Eisenstein

$D = 3^6 \cdot 7^2$ is a square

$\Longrightarrow$ Gal $\cong A_3$.

$\square$

Constructing a family of poly / $\mathbb{Q}$ with Galois group A_3 $\overset{?}{\Longleftrightarrow}$

$\Longleftrightarrow$ rat'l solutions to $y^2 = -4A^3 - 27B^2$

For a fixed B, this is an elliptic curve.

The rational points of an elliptic curve form an abelian group

If $B = 7$, sol'n $(3^3 \cdot 7, -21) = (y, A)$

Turns out, this sol'n has infinite order

$\overset{?}{\Longrightarrow}$ $\exists$ ∞'ly many cubic extensions of $\mathbb{Q}$ with Galois group A_3.