Abstract Algebra

キャプテン・ムラサ

Basic definition

$f: A \to B$ is a function $\Leftrightarrow$

$\forall x \in A, \exists! y \in B$ s.t. $y = f(x)$ $(x, y) \in f$ where $f \subseteq A \times B$

$f: A \to B$ injective (one-to-one) $\Leftrightarrow$

$\forall x, y \in A$, if $f(x) = f(y)$, then $x = y$

$f: A \to B$ sujective (onto) $\Leftrightarrow$

$\forall y \in B, \exists x \in A$ s.t. $y = f(x)$

$f: A \to B$ bijective $\Leftrightarrow$

f is both injective and sujective

$f: X \to Y$ invertible $\Leftrightarrow$

$\exists\, g: Y \to X$, s.t. $g \circ f = id_X$, $f \circ g = id_Y$

Thm. f is invertible $\Leftrightarrow$ f is bijective

proof: Choose $y \in Y$ arbitarily, then $\exists! x$ s.t. $y = f(x)$

Also, $\forall x \in X, \exists! y \in Y$, s.t. $y = f(x)$

so $\exists\, g: Y \to X$, $g \circ f = id_X$, $f \circ g = id_Y$

Def. $(S, \leq)$ is a partially ordered set $\Leftrightarrow$

{ ① $\forall a \in S$, $a \leq a$

② if $a \leq b$, $b \leq a$, then $a = b$

③ if $a \leq b$, $b \leq c$, then $a \leq c$

幽霊客船の時空を越えた旅

Ex.1 Every vector space has a basis

Let C be a chain of linearly independent sets ordered by "$\subseteq$"

Check Every chain has an upper bound

Let C be a chain of linearly independent sets

$\bigcup C$ is linearly independent

Thus $\bigcup C$ is an upper bound of C ✓

Therefore every chain has an upper bound.

$\exists$ a maximal linearly independent set B

For all other linearly independent set A $B \nsubseteq A$

Suppose B is not a basis, then $\exists \vec{v}$ s.t. $B \subseteq B \cup \{v\}$, which contradicts

Ex.2 Every set A can be well-ordered

$a_1 \to a_1 < a_2 \longrightarrow a_1 < a_2 < a_3$

① Identify the partially ordered set

Pairs $(S, \leq_S)$ such that "$\leq_S$" well-orders S

Define: $(S, \leq_S) \leq (T, \leq_T)$ if:

- $S \subseteq T$
- If $a \leq_S b$, then $a \leq_T b$
- If $b \in T - S$ and $a \in S$, then $a \leq_T b$

Check. Every set has an upper bound

Let C be a chain of these pairs

$(\bigcup\{S \mid (S, \leq_S) \in C\}, a \leq b$ if $a \leq_S b$ for some $(S, \leq_S) \in C)$

thus this an upper bound for those pairs ✓

Therefore $\exists$ maximal pair $(W, \leq_W)$

i.e. $\forall (B, \leq_B)$, $(W, \leq_W) \nleq (B, \leq_B)$

Assume that $W \neq A$

There exist a value c such that $c \notin W$

$(W, \leq_W) \leq (W \cup \{c\}, a \leq_W b$ or $a \leq c)$. contradicts

Def. $(S, \leq)$ is a totally ordered set $\Leftrightarrow$

{ ① $(S, \leq)$ is a partially ordered set

② $\forall a, b \in S$, either $a \leq b$ or $b \leq a$

Axiom of Choice

For a set of none-empty set $\{S_i\}_{i \in I}$, $\exists (x_i)_{i \in I}$, s.t. $\forall i \in I$, $x_i \in S_i$

Zorn's Lemma

In a partially ordered set, if every chain has an upper bound, then the set has a maximal element.

proof: Assume $(P, <)$ has no maximal element

$\Rightarrow$ For every $x \in P$, there exists $y \in P$ s.t. $x < y$

By the Axiom of Choice, $\exists f: P \to P$ s.t. $x < f(x)$ for all $x \in P$

Construct a strictly increasing sequence $(x_\alpha)_{\alpha \in A}$

Choose x_0 arbitarily from P, define $x_\alpha = f(x_\beta)$, $\alpha = \beta + 1$

Since $x_\beta < f(x_\beta)$, we have $x_\beta < x_\alpha$

Consider the chain $C_\lambda = \{x_\beta \mid \beta < \lambda\}$

By hypothesis, C_λ has an upper bound $u_\lambda \in P$

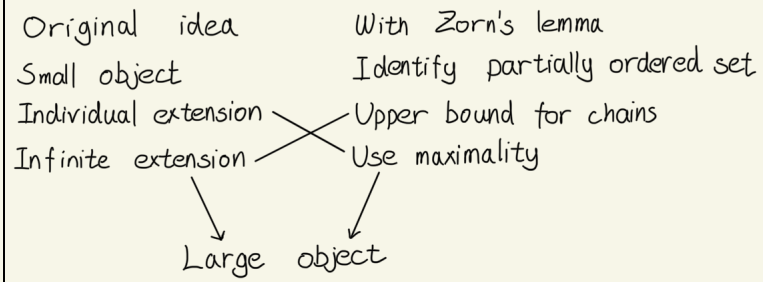
Define $x_\lambda = f(u_\lambda)$. For all $\beta < \lambda$, $x_\beta \leq u_\lambda < f(u_\lambda) = x_\lambda$

Thus $(x_\alpha)_{\alpha \in A}$ is strictly increasing

$\exists$ an injective map $\phi: A \to P$, where $\phi(\alpha) = x_\alpha$

However, A is a proper class, thus ϕ can't be injective

Therefore it contradicts, the lemma holds



Chaper 1

Group Theory

Ex1. Abel Group

$(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$

①	✓	✓	✓	✓
②	0 ✓	0 ✓	0 ✓	0 ✓
③	$-a$ ✓	$-\frac{p}{q}$ ✓	$-a$ ✓	$-a-bi$ ✓
④	✓	✓	✓	✓

Ex2. $(\mathbb{N},+)$ is not a group

proof: Assume $a+1=0$, $a=-1\notin\mathbb{N}$

Ex3 $(\mathbb{R},\cdot)$ is not a group

There exist no $a\in\mathbb{R}$, s.t. $a\cdot 0=1$

$(\mathbb{R}^{\times}=\mathbb{R}\setminus\{0\},\cdot),(\mathbb{Q}\setminus\{0\},\cdot)$

①	✓	✓
②	1 ✓	1 ✓
③	$\frac{1}{a}$ ✓	$\frac{q}{p}$ ✓
④	✓	✓

Ex.4: $(\mathbb{Z}\setminus\{0\},\cdot)$ is not a group

$\forall\, n\in\mathbb{Z}$, $1\cdot n=n\cdot 1=n$

However $\forall\, n>1$, $n\cdot\frac{1}{n}=1$, $\frac{1}{n}\notin\mathbb{Z}$

Ex.5

$S_X=\{f: X\to X, \text{bijective}\}$, $X\neq\emptyset$

$(S_X,\circ)$ is a group

① $f\circ g: X\to X$, $g\circ f: X\to X$

② $f\circ(g\circ h)=(f\circ g)\circ h$

③ $id_x\circ f=f\circ id_x=f$

④ Since f is bijective, then f is invertible

$\exists f^{-1}$, $f\circ f^{-1}=f^{-1}\circ f=id_X$

Group

"$\cdot$" is a binary operation on S <=>

$\cdot: S\times S\to S$ e.g. $\cdot(a,b)=a\cdot b$

Def. $(G,\cdot)$ is a group <=>

① $\forall\, a,b,c\in G$, $a\cdot(b\cdot c)=(a\cdot b)\cdot c$

② $\exists e\in G$, $\forall\, a\in G$, $a\cdot e=e\cdot a=a$

③ $\forall\, a\in G$, $\exists\, a^{-1}\in G$, $a\cdot a^{-1}=a^{-1}\cdot a=e$

④ $\forall\, a,b\in G$, $ab, ba\in G$

Def. $(G,+)$ is an Abel group <=>

① $\forall\, a,b,c\in G$, $a+(b+c)=(a+b)+c$

② $\exists e\in G$, $\forall\, a\in G$, $a+e=e+a=a$

③ $\forall\, a\in G$, $\exists\,(-a)\in G$, $a+(-a)=(-a)+a=e$

④ $\forall\, a,b\in G$, $a+b=b+a\in G$

Prop. Let $(G,\cdot)$ be a group, then:

(1) e is unique

(2) for every $a\in G$, a is unique

(3) $ax=b$ <=> $x=a^{-1}b$: $a^{-1}ax=a^{-1}b \Rightarrow x=a^{-1}b$

(4) $xa=b$ <=> $x=ba^{-1}$: $xaa^{-1}=ba^{-1}\Rightarrow x=ba^{-1}$

(5) $axb=c$ <=> $x=a^{-1}cb^{-1}$: $a^{-1}axbb^{-1}=a^{-1}cb^{-1}\Rightarrow x=a^{-1}cb^{-1}$

proof: (1) Assume $e_1,e_2\in G$

$e_1=e_1e_2=e_2 \Rightarrow e$ is unique

(2) Assume $ab=ac=e$

$b=be=bac=ec=c \Rightarrow a^{-1}$ is unique

Linear Group

$GL_n(\mathbb{R})=\{A\in\mathbb{R}^{n\times n},\ \det(A)\neq 0\}$

$(GL_n(\mathbb{R}),\cdot)$ is a group, but not Abel

① $\det(A)\neq 0$, $\det(B)\neq 0$, $\det(AB)=\det(A)\det(B)\neq 0$

② $AI=IA$, $\det(AI)=\det(A)\neq 0$

③ $AA^{-1}=A^{-1}A=I$, $\det(AA^{-1})=1\neq 0$

④ $(AB)C=A(BC)$, $\det(ABC)\neq 0$, so it is a group

Yet $\det(A+(-A))=0$

so it is not Abel

Special Linear Group

$SL_n(\mathbb{R})=\{A\in\mathbb{R}^{n\times n},\ \det(A)=1\}$

$(SL_n(\mathbb{R}),\cdot)$ is a group, but not abel

① $\det(A)=1$, $\det(B)=1$, $\det(AB)=1$

② $\det(AB)=\det(BA)$

③ $AA^{-1}=A^{-1}A=I$, $\det(I)=1$

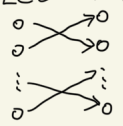
④ $A(BC)=(AB)C$

Ex.6

$S_n = \{f : \{1, \cdots, n\} \to \{1, \cdots, n\}, \text{bij.}\}$

$(S_n, \circ)$ is a group

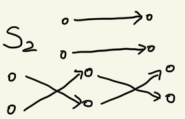
Let $X = \{1, \cdots, n\}$, ✓



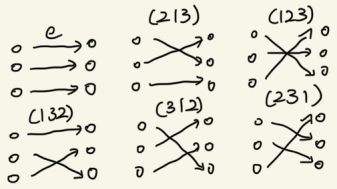
$|S_n| = n!$

S_1  Trivial Group

$S_1 = \{e\}$ $\quad id \circ id = id$, $id^{-1} = id$

S_2  , so $S_2 = \{e, (12)\}$

$\circ$	e	(12)
e	e	(12)
(12)	(12)	e

S_3 

Def. if $(G, \cdot)$ is a group, then $H < G$

$\Leftrightarrow$ H is a subgroup of G $\Leftrightarrow$ $H \subset G$ and $(H, \cdot)$ is a group

Thm. $H < G \Leftrightarrow$

① $\forall a, b \in H$, $a \cdot b \in H$ (closed under multiplication)

② $e \in H$

③ $\forall a \in H$, $a^{-1} \in H$

if $H < G$, $(H, \cdot)$ is a group. $H \subset G$

① ✓ ②: $\forall a \in H \subset G$, $ae = ea = a$, since e is identical, $e \in H$

③ $aa^{-1} = a^{-1}a = e$ for $\forall a \in H$, since a^{-1} is identical in G, so $a^{-1} \in H$

Thm. $(n\mathbb{Z}, +) < (\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$

proof: $n\mathbb{Z} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Also, they are all groups, so the theorem holds

Thm. $(SL_n(\mathbb{R}), \cdot) < (GL_n(\mathbb{R}), \cdot)$

proof: $SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$ while they are both groups

Ex1.

If $H<G$

Let $j: H \longrightarrow G$ be the inclusion (嵌入) given by $j(a)=a$ for every $a \in H$, then $j: H \xrightarrow{Hom} G$

proof: $j(ab)=ab=j(a)j(b)$

Ex2.

If $(G,\cdot)$ is a group, $id_G: G \xrightarrow{Hom} G$

proof: $G \subseteq G$, from Ex1, it's done

Ex3.

$\det: (GL_n(\mathbb{R}),\cdot) \xrightarrow{Hom} (\mathbb{R}^\times,\cdot)$

proof: $\det(AB)=\det(A)\det(B)>0$

Def. Given two groups $(G,\cdot)$, $(G',\cdot)$

$f: G \to G'$ is homomorphism (同态) $\iff f: G \xrightarrow{Hom} G'$

$\iff \forall a,b \in G$, $f(a\cdot b)=f(a)\cdot f(b)$

"$\cdot$" in G "$\cdot$" in G'

Prop. If $f: G \xrightarrow{Hom} G'$, then:

① $f(e)=e'$ $(e' \in G')$

② $\forall a \in G$, $f(a^{-1})=f(a)^{-1}$

Proof: ① $f(e)=f(ee)=f(e)f(e)$, since $f(e) \in G'$

then $f(e)=e'$

② Let $a \in G$ (inverse element is unique)

$f(a)f(a^{-1})=f(aa^{-1})=f(e)=e'$

so $f(a^{-1})=f(a)^{-1}$

Def. If $f: G \xrightarrow{Hom} G'$, then $Ker(f)=\{a \in G : f(a)=e'\}$

$Im(f)=\{f(a) : a \in G\}$

Thm. If $f: G \xrightarrow{Hom} G'$, $Ker(f)<G$ and $Im(f)<G'$

proof: (1) ① if $a,b \in Ker(f)$, $f(a)=f(b)=e'$, $f(ab)=f(ba)=e'$, $ab \in Ker(f)$

② $f(e)=e'$, $e \in Ker(f)$

③ $f(a^{-1})=f(a)^{-1}=e'^{-1}=e'$, $a^{-1} \in Ker(f)$

(2) ① $f(a)f(b)=f(ab)=f(ba)=f(b)f(a)$ (G is a group), $f(a)f(b) \in Im(f)$

② $f(a)f(e)=f(e)f(a)$, $e' \in Im(f)$

③ $f(a)f(a)^{-1}=f(a)f(a^{-1})=e'=f(a^{-1})f(a)=f^{-1}(a)f(a)$, $f(a)^{-1} \in Im(f)$

$\exists f: (\mathbb{R}, +) \xrightarrow[\text{bij.}]{\text{Hom}} (\mathbb{R}_{++}, \cdot)$

Notice that $f(x) = e^x$

$\exists g: (\mathbb{R}_{++}, \cdot) \xrightarrow[\text{bij.}]{\text{Hom}} (\mathbb{R}, +)$

Notice that $g(x) = \ln x$

$$(\mathbb{R}_{++}, \cdot) < (\overset{\mathbb{R}/\{0\}}{\overset{\shortparallel}{\mathbb{R}^\times}}, \cdot)$$

① $a>0, b>0 \Rightarrow ab>0$

② $a \cdot 1 = 1 \cdot a = a$

③ $a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$

Ex. $(\{1, -1, i, -i\}, \cdot) \cong$
$(\{\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \begin{pmatrix} -1 & \\ & -1 \end{pmatrix}, \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}, \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}\}, \cdot)$

Ex. Fix $v \in \mathbb{R}^n \setminus \{0\}$, $F = \mathbb{R}$

$(\mathbb{R}, +) \cong (\text{span}(v), +) < (\mathbb{R}^n, +)$

proof: $cv + dv = (c+d)v$

$0 \cdot v = v \cdot 0 = 0$

$v + (-v) = (-v) + v = 0$

$\text{span}(v) \subset \mathbb{R}^n$

so $(\text{span}(v), +)$ is a group

let $f(c) = cv : \mathbb{R} \to \text{span}(v)$

Ex. Fix $\mathbb{R}^n$, $F = \mathbb{R}$

$S = \{v_1, \cdots, v_k\}$, linearly independent

Then $(\mathbb{R}^k, +) \cong (\text{span}(S), +) < (\mathbb{R}^n, +)$

let $f(a) = a_1 v_1 + \cdots + a_k v_k : \mathbb{R}^k \to \text{span}(S)$

Def. f is surjective homomorphism $\Leftrightarrow f: G \xrightarrow[\text{surj.}]{\text{Hom}} G'$

f is injective $\sim \Leftrightarrow f: G \xrightarrow[\text{inj.}]{\text{Hom}} G'$

f is bijective $\sim \Leftrightarrow f: G \xrightarrow[\text{bij.}]{\text{Hom}} G'$

Thm. if $f: G \xrightarrow{\text{Hom}} G'$, then

f is injective $\Leftrightarrow \ker(f) = \{e\}$

proof: ① If f is injective, $f(e) = e'$

if $f(a) = e'$, then $f(a) = f(e) = e'$, $a = e$, so $\ker(f) = \{e\}$

② If $\ker(f) = \{e\}$, let $f(a) = f(b)$, $f(a)f(a)^{-1} = f(b)f(a)^{-1}$

then $f(ba^{-1}) = e'$, then $ba^{-1} = e$

Since the inverse element is unique, then $a = b$

so f is injective

Def. $f: G \to G'$ is isomorphism (同构) $\Leftrightarrow f: G \xrightarrow{\text{iso}} G'$

$\Leftrightarrow$ ① f is bijective

② $f: G \xrightarrow{\text{Hom}} G'$

③ $f^{-1}: G' \xrightarrow{\text{Hom}} G$

Def. $G \cong G' \Leftrightarrow \exists f: G \xrightarrow{\text{iso}} G'$

Thm. $f: G \xrightarrow{\text{iso}} G' \Leftrightarrow f: G \xrightarrow[\text{bij.}]{\text{Hom}} G'$

proof "$\Rightarrow$" is from the definition

"$\Leftarrow$": Since f is bijective, then $f^{-1}: G' \to G$ exist

$\forall c, d \in G'$, $\exists! a, b \in G$, $c = f(a)$, $d = f(b)$

$f^{-1}(cd) = f^{-1}(f(a)f(b)) = f^{-1} \circ f(ab) = ab = f^{-1}(c) f^{-1}(d)$

Generalised

V is a vector space. F is a scalor field

$\{v_1, \cdots, v_n\}$ is linearly independent

then $(F^n, +) \cong (\text{span}(v_1, \cdots, v_n), +)$

$f: F^n \longrightarrow \text{span}(v_1, \cdots, v_n)$

$a = (a_1, a_2, \cdots, a_n)$, $b = (b_1, b_2, \cdots, b_n)$

$f(a) = a_1 v_1 + \cdots + a_n v_n$ $f(a+b) = f(a) + f(b)$. so f is homo.

Also $f^{-1}: \text{span}(v_1, \cdots, v_n) \to F^n$, $f^{-1}(a_1 v_1 + \cdots + a_n v_n) = (a_1, \cdots, a_n)$

$f^{-1}(x+y) = f^{-1}((a_1+b_1)v_1 + \cdots + (a_n+b_n)v_n) = (a_1+b_1, \cdots, a_n+b_n) = f^{-1}(x) + f^{-1}(y)$, so f is iso.

Thm. If $f: G \xrightarrow{iso} G'$, then

① $|G'| = |G|$ (cardirality)

② $H < G \iff f(H) < G'$

③ If G'' is a group, then,

$\exists\, g: G' \xrightarrow{Hom} G'' \iff \exists\, g': G \xrightarrow{Hom} G''$

$\exists\, g: G' \xrightarrow{iso} G'' \iff \exists\, g': G \xrightarrow{iso} G''$

(proof)

(1) $f: G \xrightarrow{iso} G' \Rightarrow f$ is bijective $\Rightarrow |G| = |G'|$

(2) $\forall\, a, b \in H$, $f(a), f(b) \in G'$

Since $a, b \in H$, H is a group, then $a^{-1}, b^{-1} \in H$

Since $H < G$, then $e \in H$, so $f(e) = e' \in f(H)$

(3) ① $g \circ f(ab) = g(f(a)f(b)) = g \circ f(a) \cdot g \circ f(b)$ ✓

② Since f, g are bijective, then $g \circ f$ is bijective

from ① we know that $g \circ f: G \xrightarrow{Hom} G''$

let $c = g \circ f(a)$, $d = g \circ f(b)$, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

$(g \circ f)^{-1}(cd) = f^{-1} \circ g^{-1}(cd) = f^{-1}(g^{-1}(c)\, g^{-1}(d)) = (g \circ f)^{-1}(c) \cdot (g \circ f)^{-1}(d)$

($g: G' \xrightarrow{iso} G''$)

Thm. If $(G, \cdot)$ a group, $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$

Thm. If $(G, \cdot)$ a group, $a_1, \cdots, a_n \in G$

then $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}$

Ex. $(n\in\mathbb{N}^*)$, find $\langle w_n\rangle$, where $w_n=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$

$\langle w_n\rangle=\{w_n, w_n^2, \cdots, w_n^{n-1}, 1\}$

Ex. if $(G,\cdot)$ is a group then $\langle e\rangle=\{e\}$

Def. if $(G,\cdot)$ a group, $a\in G$, $n\in\mathbb{N}^*$

then $\begin{cases} a^n=a\cdots a, \text{ with } n \text{ a's} \\ a^{-n}=(a^n)^{-1} \end{cases}$. Also $a^0=e$

Collary. If $(G,\cdot)$ a group, Fix $a\in G$

then $f:(\mathbb{Z},+)\xrightarrow{\text{Hom}}(G,\cdot)$ given by $f(n)=a^n$

proof: $f(m+n)=a^{m+n}=a^m\cdot a^n=f(m)\cdot f(n)$

Collary. $\{a^n: n\in\mathbb{Z}\}<G$, define $\langle a\rangle=\{a^n: n\in\mathbb{Z}\}$

Def. G is cyclic if $G=\langle a\rangle$

Thm. If $(G,\cdot)$ is a group, $a,b\in G$, then

$\langle a\rangle<\langle b\rangle \Leftrightarrow a\in\langle b\rangle$

proof: "$\Rightarrow$" $a\in\langle a\rangle\subset\langle b\rangle$ ✓

"$\Leftarrow$" $a\in\langle b\rangle$, then $a=b^m$, $a^n=b^{mn}\in\langle b\rangle$, so $\langle a\rangle\subset\langle b\rangle$

Since $e\in\langle a\rangle$, then $\langle a\rangle<\langle b\rangle$

Def. if $(G,\cdot)$ is a group, $a\in G$

then $|a|=\begin{cases} \min\{n\in\mathbb{N}^*, a^n=e\}, & \text{if } \exists n\in\mathbb{N}^*, a^n=e \\ \infty, & \text{otherwise} \end{cases}$

Ex1 $|\langle \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} \rangle| = 4$

$|\langle \begin{pmatrix} -1 & \\ & -1 \end{pmatrix} \rangle| = 2$

Ex2. Prove: $|\langle 1+2i \rangle| = \infty$

$\|1+2i\| = \sqrt{5}$, $\|1+2i\|^n = (\sqrt{5})^n$

so $(1+2i)^m = (1+2i)^n$ only if $m=n$

so $|\langle 1+2i \rangle| = \infty$

$\langle i \rangle \simeq \langle \begin{bmatrix} -1 & \\ & 1 \end{bmatrix} \rangle \simeq \langle -i \rangle \simeq \langle \begin{bmatrix} -1 & \\ & 1 \end{bmatrix} \rangle$

$|\langle i \rangle| = |\begin{bmatrix} -1 & \\ & 1 \end{bmatrix}| = |-i| = |\begin{bmatrix} -1 & \\ & 1 \end{bmatrix}| = 4$

so they are isomorphic

Ex.1 $(\mathbb{Z}, +)$, $\mathbb{Z} = \langle 1 \rangle$

& $|1| = |\mathbb{Z}| = \infty$

$\mathbb{Z} = \{\cdots, -1, 0, 1, \cdots\}$

Ex2. if V is a vector space over $\mathbb{R}/\mathbb{C}$, if $v \neq 0$, then $|v| = \infty$

Ex3: $-(\mathbb{Z}, +)$ if $n \in \mathbb{N}^*$

then $n\mathbb{Z} = \langle n \rangle = \{nk : k \in \mathbb{Z}\}$

$\{\cdots, -2, -1, 0, 1, 2, \cdots\}$

$\{\cdots, -2k, -k, 0, k, 2k, \cdots\}$

Def. if $(G, \cdot)$ is a group, $a \in G$

then $|a| = \begin{cases} \min\{n \in \mathbb{N}^*, a^n = e\}, & \text{if } \exists n \in \mathbb{N}^*, a^n = e \\ \infty, & \text{otherwise} \end{cases}$

Def. G is cyclic $\Leftrightarrow \exists a \in G$, $G = \langle a \rangle$

Recall: $|(G, \cdot)| = |G|$

Thm. if $G = \langle a \rangle$, then $|G| = |a|$

proof: ① if $|a| = \infty$, $\forall n \in \mathbb{N}^+$, $a^n \neq e$, $a^m = a^n \Rightarrow m = n$

then $G = \langle a \rangle = \{\cdots, a^{-1}, e, a, \cdots\}$, so $|G| = |\mathbb{N}| = |a|$

② if $|a| \neq \infty$, it is trivial

Thm. If $G = \langle a \rangle$, $G' = \langle a' \rangle$, $|a| = |a'|$, then $G \simeq G'$

proof: $G = \{\cdots, a^{-1}, e, a, \cdots\}$, $G' = \{\cdots, a'^{-1}, e', a', \cdots\}$

then let $f: G \to G'$, $f(a^n) = a'^n$, $f^{-1}: G' \to G$, $f^{-1}(a'^n) = a^n$

$f(a^m \cdot a^n) = a'^{m+n} = a'^m \cdot a'^n = f(a^m) f(a^n)$, $f^{-1}(a'^m \cdot a'^n) = a^{m+n} = f^{-1}(a'^m) f^{-1}(a'^n)$

so $G \simeq G'$

Thm. If $G \simeq G'$, $G = \langle a \rangle$, $f: G \xrightarrow{\text{iso}} G'$, then $|f(a)| = |a|$

proof: if $|a| = n$, $f(a)^n = f(a^n) = f(e) = e'$

so $|f(a)| \leq |a|$.

Since $f: G \xrightarrow{\text{iso}} G'$, then let $b = f(a)$, $a = f^{-1}(b)$, if $|b| = m$

$f^{-1}(b)^n = f^{-1}(b^n) = f^{-1}(e') = e$, so $|f^{-1}(b)| \leq |b| \Leftrightarrow |a| \leq |f(a)|$

so $|f(a)| = |a|$

Additionally cyclic group

$(G, \cdot)$ group, Fix $a \in G$

if $n \in \mathbb{N}^*$ $\begin{cases} na = a + \cdots + a, \text{ with } n \text{ } a\text{'s} \\ (-n)a = -(na) \\ 0a = 0 = e \end{cases}$

Also $\forall m, n \in \mathbb{Z}$, $(m+n)a = ma + na$, $\langle a \rangle = \{na, n \in \mathbb{Z}\}$

$\exists f: (\mathbb{Z}, +) \xrightarrow{\text{Hom}} (G, +)$ given by $f(n) = na$

Since $f(m+n) = (m+n)a = ma + na = f(m) + f(n)$

Ex 1:
$\mathbb{Q}^\times < \mathbb{R}^\times$, $\pi\mathbb{Q}^\times = \{\pi\frac{p}{q} : p, q \in \mathbb{Z}^\times\}$

Def. if $H<G$, $a\in G$, then $aH=\{ah : h\in H\}$ & $Ha=\{ha : h\in H\}$

Check. $a\in aH$

if $H<G$, $h\in H$, then $hH=H$

Cor. if $H<G$, then $eH=H$

Thm. if $(G,\cdot)$ is a group, $H<G$, then

$aH=bH \Leftrightarrow a\in bH \Leftrightarrow b\in aH$

proof: $\{ah : h\in H\}\subseteq\{bh : h\in H\}$, since $e\in H$, then $ae=a\in bH$

Similarly, $be=b\in aH$

Cor. $aH=eH \Leftrightarrow a\in H \Leftrightarrow e\in aH$

Cor. if $H<G$, $a\in G$, then $aH<G \Leftrightarrow a\in H$

proof: $\Rightarrow$ if $aH<G$ then $\{ah : h\in H\}\subseteq G$

$(ah_1)(ah_2)\subseteq aH$, Let $(ah_1)(ah_2)=ah_3$, then $a^2h_1h_2=ah_3$

so $a=h_3h_2^{-1}h_1^{-1}\in H$

$\Leftarrow$: if $a\in H$, then $\forall h\in H$, $ah\in H$, so $aH<G$

Cor. if $H<G$, then $a\sim b \Leftrightarrow aH=bH$

Thm. if $H<G$, $a\in G$,

then $\exists f: H \xrightarrow{bij} aH$ (not homomorphic)

given by $f(h)=ah$

Check. $f^{-1}(k)=a^{-1}k$

If $H<G$, then $H=HH$, "$\supset$" $h=he\in HH$ ✓

"$\subset$" $h_1h_2\in H$ ✓

Cor. if $H<G$, $a\in G$, then $|aH|=|H|$

proof: $aH=\{ah_1, ah_2, \cdots, ah_n\} \underline{\vee} \{h_1, h_2, \cdots, h_n\}$

Cor. (By Lagrange) if $H<G$, G is finite, then $[G:H]=\frac{|G|}{|H|}$

proof: $G=\bigcup_{a\in G} aH=\bigsqcup_{i=1}^{n} a_iH$, so $|G|=|\bigsqcup_{i=1}^{n} a_iH|=\sum_{i=1}^{n}|a_iH|=n|H|$

so $[G:H]=\frac{|G|}{|H|}$

(Here $[G:H]=|\{gH \mid g\in G\}|$

Prop. if $H_1, H_2, H_3 \subset G$, $a, b\in G$, $h_i\in H_i$, then

(1) $H_1(H_2H_3)=(H_1H_2)H_3$

$h_1(h_2h_3)=(h_1h_2)h_3$

(2) $a(H_1H_2)=(aH_1)H_2$

$a(h_1h_2)=(ah_1)h_2$

(3) $(H_1a)H_2=H_1(aH_2)$

$(h_1a)h_2=h_1(ah_2)$

(4) $(H_1H_2)a=H_1(H_2a)$

$(h_1h_2)a=h_1(h_2a)$

(5) $(H_1a)b=H_1(ab)$

$(h_1a)b=h_1(ab)$

(6) $(aH_1)b=a(H_1b)$

$(ah_1)b=a(h_1b)$

(7) $(ab)H_1=a(bH_1)$

$(ab)h_1=a(bh_1)$

Def. N is a normal subgroup $\Leftrightarrow N\triangleleft G$

$\Leftrightarrow N<G$ & $\forall a\in G$, $aN=Na$

Thm. if $N\triangleleft G$, then $(aN)(bN)=(ab)N$

proof: $(aN)(bN)=aNNb=aNb=abN$ ✓

if $H<G$, $H=HH$

"$\supset$" $h=he\in HH$ ✓

"$\subset$" $h_1h_2\in H$ ✓

Fermat's Little Thm

Suppose $p \in \mathcal{P}$, then for $\forall\, a \in \mathbb{N}^*$, $a^{p-1} \equiv 1 \pmod p$

proof: Let $G = \{\bar{0}, \bar{1}, \cdots, \overline{p-1}\}$

where $\bar{a} \cdot \bar{b} := \overline{ab} \pmod p$

Then consider the subgroup $H = \langle a \rangle$, by Lagrange Thm,

$|H| \mid |G|$, However $|G| \in \mathcal{P}$, so $|H| = 1$ or $|H| = p$

if $|H| = 1$, then $a = \bar{0}$.

Otherwise, $a^p = a$, so $a^{p-1} = 1$ i.e. $a^{p-1} \equiv 1 \pmod p$

Lemma. If G is a group, $A \lhd G$, $B < G$, then $AB < G$

pf) $\forall\, ab \in AB$, $b^{-1}a^{-1} = cb^{-1}$ for some $c \in A$. then $b^{-1}a^{-1} \in AB$

Thus $AB < G$

Lemma. If $A \lhd G$, $B < G$, then $|AB| = \dfrac{|A||B|}{|A \cap B|}$

pf) Consider the left caset. Define $\pi : B \to (AB)/A$, $b \mapsto Ab$

Then $\ker(\pi) = A \cap B$, $\operatorname{im}(\pi) = (AB)/A$

Thus $B/(A \cap B) \cong (AB)/A$

Therefore $\dfrac{|B|}{|A \cap B|} = \dfrac{|AB|}{|A|}$, $|AB| = \dfrac{|A||B|}{|A \cap B|}$

Def. if $N \lhd G$, then $G/N = \{aN, a \in G\}$

define "$\cdot$" on G/N as product of sets

(*) **Check. well-defined**

if $aN = cN$, $bN = dN$. WTS $(ab)N = (cd)N$

Thm. $(G/N, \cdot)$ is a group, which is called the quotient group (G mod N)

proof: ⓪ $(aN)(bN) = (bN)(aN) = (ab)N \in G/N$ ✓

① $(aN)(bNcN) = (aNbN)(cN)$ ✓

② $(aN)N = N(aN) = aN$ ✓

③ $(aN)(a^{-1}N) = (a^{-1}N)(aN) = N$ ✓

Lemma. if $H_1, H_2 \subset G$, $a \in G$, then

① $aH_1 = H_2b \Leftrightarrow aH_1b^{-1} = H_2 \Leftrightarrow a^{-1}H_2b = H_1$

② $aH_1 = bH_2 \Leftrightarrow b^{-1}aH_1 = H_2 \Leftrightarrow a^{-1}bH_2 = H_1$

proof:

① $\{ah_1 : h_1 \in H_1\} = \{h_2b : h_2 \in H_2\}$

(1) $\forall\ h_1 \in H_1$, $ah_1 \in \{h_2b : h_2 \in H_2\}$ so $ah_1b^{-1} \in H_2$ for $\forall\ h_1 \in H_1$

$h_2b \in \{ah_1 : h_1 \in H_1\}$ so $h_2 \in aH_1b^{-1}$ for $\forall\ h_2 \in H_2$

so $aH_1b^{-1} = H_2$

(2) $ah_1 = h_2b$, $h_1 = a^{-1}h_2b$, so $a^{-1}h_2b \in H_1$ for $\forall\ h_2 \in H_2 \Rightarrow a^{-1}H_2b \subset H_1$

$h_1 \in a^{-1}H_2b$ for $\forall\ h_1 \in H_1$, so $H_1 \subset a^{-1}H_2b$.

so $a^{-1}H_2b = H_1$

②: ~

Cor. $aH=Ha \Leftrightarrow aHa^{-1}=H \Leftrightarrow a^{-1}Ha=H$

Lemma. $N \lhd G \overset{def}{\Leftrightarrow} \forall a \in G,\ Na=aN$

$\overset{check}{\Leftrightarrow} \forall a \in G, \forall k \in N,\ aka^{-1} \in N$

Thm. if $f: G \xrightarrow{Hom} G'$, then $Ker(f) \lhd G$

proof: $Ker(f)=\{a : f(a)=e'\}$, $f(ab)=f(a)f(b)$ for $\forall\ a,b \in G$

Obviously $Kef(f) < G$, and $cKer(f)=\{ck : k \in Ker(f)\}$

$\forall c \in G$, $f(ckc^{-1})=f(c)f(k)f(c^{-1})=f(c)f(c^{-1})=f(e)=e'$, so $ckc^{-1} \in ker(f)$

so $Ker(f) \lhd G$

☆ Thm. (The first isomorphism theorem)

if $f: G \xrightarrow{Hom} G'$, then $G/Ker(f) \cong Im(f)$

proof: $G/Ker(f)=\{aKer(f) : a \in G\}$

Notice that $f(aKer(f))=\{f(a)\}$ for $\forall a \in G$

let $\hat{f}(aKer(f))=f(a)$

$\hat{f}(aKer(f)\,bKer(f))=\hat{f}(abKer(f))=f(ab)=f(a)f(b)=\hat{f}(aKer(f))\hat{f}(bKer(f))$

so $\hat{f}: G/Ker(f) \xrightarrow{Hom} Im(f)$

Also notice that $\hat{f}^{-1}(a)=aKer(f)$ is homomorphic

so $G/Ker(f) \cong Im(f)$

If $f: G \xrightarrow{hom} H$, $ker(f)=\{e\}$, then f is one-to-one

pf) If $f(a)=f(b)$, then $f(a)^{-1}=f(b)^{-1}$

$f(a)f(a^{-1})=f(e)=f(a)f(b)^{-1}=f(ab^{-1})$

so $a=b$

Ex. $n\mathbb{Z} \lhd \mathbb{Z}$

Notice that $(\mathbb{Z}, +)$ is Abelian while $n\mathbb{Z} < \mathbb{Z}$

$(\mathbb{Z}_n, +)$ is a group

$\mathbb{Z}_n = \{\bar{0}, \cdots, \overline{n-1}\}$

$\bar{a} + \bar{b} = \overline{(a+b) \bmod n}$ (defined)

Ex.

$\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$\bar{1} + \bar{4} = \overline{5 \bmod 5} = \bar{0}$ $\quad \bar{2} + \bar{2} = \overline{4 \bmod 5} = \bar{4}$

$\bar{3} + \bar{4} = \overline{7 \bmod 5} = \bar{2}$

Check. $\mathbb{Z} = \langle \bar{1} \rangle$

proof: $\bar{1} + \bar{1} + \cdots + \bar{1} = \overline{n \bmod n} = \bar{0}$

Thm. if $(G, \cdot)$ is a group, then $\{e\} \lhd G$, $G \lhd G$

proof is trivial

Thm. if $(G, \cdot)$ is an Abelian group

then $H < G \iff H \lhd G$

proof: "$\Leftarrow$" $\surd$, from definition

"$\Rightarrow$" Since $(G, \cdot)$ is Abelian, then $ab = ba$ for $\forall a, b \in H$

$aH = \{ab : b \in G\} = \{ba : b \in G\} = Ha$, so $aH = Ha \Rightarrow H \lhd G$

Thm. if $(G, \cdot)$ is a group, then $\begin{cases} G/\{e\} \simeq G \\ G/G \simeq \{e\} \end{cases}$

proof: ① $G/\{e\} = \{\{a\} : a \in G\}$

let $f(a) = a$ for $\forall a \in G$, Notice that $f: G \xrightarrow{\text{Hom}} G$

$\ker(f) = \{e\}$, $\mathrm{Im}(f) = G$, so $G/\{e\} \simeq G$

② $G/G = \{G\}$

let $g(a) = e$ for $\forall a \in G$, Notice that $g: G \xrightarrow{\text{Hom}} \{e\}$

$\ker(g) = G$, $\mathrm{Im}(g) = \{e\}$, so $G/G \simeq \{e\}$

Thm. $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^\times$

proof: Notice that $\det: GL_n(\mathbb{R}) \to \mathbb{R}^\times$ defined by $\det(A)$

then $\mathrm{Im}(\det) = \mathbb{R}^\times$, $\ker(\det) = SL_n(\mathbb{R})$

so $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^\times$

Example

$3 \equiv -7 \pmod{10}$, $3-(-7)=10 \in 10\mathbb{Z}$

$1 \equiv 7 \pmod{3}$, $1-7=-6 \in 3\mathbb{Z}$

Ex.1 $n\mathbb{Z} \lhd \mathbb{Z}$

$a \equiv b \pmod{n\mathbb{Z}} \Leftrightarrow (-a)+b \in n\mathbb{Z}$

$\Leftrightarrow a-b \in n\mathbb{Z}$

Ex.2 $\mathbb{Z} \lhd \mathbb{R}$

$a, b \in \mathbb{R}$, $a \equiv b \pmod{\mathbb{Z}}$

$\Leftrightarrow a-b \in \mathbb{Z} \Leftrightarrow (-a)+b \in \mathbb{Z}$

Ex.3 $\mathbb{Q}^\times \lhd \mathbb{R}^*$

$a \equiv b \pmod{\mathbb{Q}^*} \Leftrightarrow a^{-1}b = \frac{b}{a} \in \mathbb{Q}^\times$

Ex.4 $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$

$A, B \in GL_n(\mathbb{R})$

$A \equiv B \pmod{SL_n(\mathbb{R})} \Leftrightarrow A^{-1}B \in SL_n(\mathbb{R})$

$\Leftrightarrow \det(A)=\det(B)$

Modular Arithuetic 模算术

Def. Fix $n \in \mathbb{N}^*$, $n \geq 2$, $a \equiv b \pmod{n}$ Congruent

$\Leftrightarrow n \mid (a-b) \Leftrightarrow \exists k \in \mathbb{Z}$, s.t. $a-b=nk$

$\Leftrightarrow a-b \in n\mathbb{Z} \Leftrightarrow a+(-b) \in n\mathbb{Z}$

$\Leftrightarrow -a+b \in n\mathbb{Z} \Leftrightarrow (-a)+b \in n\mathbb{Z}$

Observation. for $a, b \in \mathbb{Z}$, $a \equiv b \pmod{n} \Leftrightarrow (-a)+b \in n\mathbb{Z} \lhd \mathbb{Z}$

& if $N \lhd G$, then $aN=bN \Leftrightarrow a^{-1}b \in N$

for $(N,+) \lhd (G,+)$, $a+N=b+N \Leftrightarrow (-a)+b \in N$

Redefine. for $a, b \in \mathbb{Z}$

$a \equiv b \pmod{n} \Leftrightarrow a+n\mathbb{Z}=b+n\mathbb{Z} \Leftrightarrow a \equiv b \pmod{n\mathbb{Z}}$

Def. if $(N,+) \lhd (G,+)$, $a, b \in G$, then $a \equiv b \pmod{N}$

$\Leftrightarrow a+N=b+N \Leftrightarrow (-a)+b \in N$

Def. if $(N,\cdot) \lhd (G,\cdot)$

$a \equiv b \pmod{N} \Leftrightarrow aN=bN \Leftrightarrow a^{-1}b \in N$

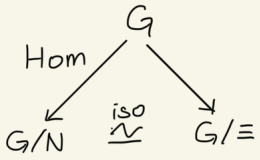
Thm. $A \equiv B \pmod{SL_n(\mathbb{R})} \Leftrightarrow \det(A)=\det(B)$

Consider. the set of equivalence classes

$G/\equiv$, i.e. $\{\bar{a} : a \in G\}$, where $\bar{a}=\bar{b} \Leftrightarrow a \equiv b \pmod{N} \Leftrightarrow aN=bN$

Def. if $\bar{a}, \bar{b} \in G/\equiv$, then $\bar{a} \cdot \bar{b} = \overline{ab}$ is well-defined

Check. "$\equiv$" is an equivalence relation



Check. $(G/\equiv, \cdot)$ is a group

$g: G/N \to G/\equiv$ is given by $g(aN) = \bar{a}$

① well-defined.

if $aN = bN$, $\bar{a} = \bar{b}$

② homomorphic. $g(aN\,bN) = g(abN) = \overline{ab} = \bar{a}\cdot\bar{b} = g(aN)\,g(bN)$

③ bijection inj. $g(aN) = \bar{e}$, $aN = eN$, $\ker(g) = \{e\}$

surj. $\forall\, \bar{a} \in G/\equiv$, $a \in G$, $g(aN) = \bar{a}$

so $G/N \simeq G/\equiv$, which means $(G/\equiv, \cdot)$ is a group

Thm. $(\mathbb{Z}, +)/(n\mathbb{Z}, +) \simeq (\mathbb{Z}_n, \oplus)$ (modular addition)

proof: Let $f(a) \equiv a \pmod n$

$f(a+b) = (a+b) \pmod n = a \pmod n \oplus b \pmod n = f(a) \oplus f(b)$

so $f: \mathbb{Z} \xrightarrow{\text{Hom}} \mathbb{Z}_n$, $\mathrm{Im}(f) = \mathbb{Z}_n$, $\ker(f) = n\mathbb{Z}$

so $(\mathbb{Z}, +)/(n\mathbb{Z}, +) \simeq (\mathbb{Z}_n, \oplus)$

Thm. $\mathbb{R}/\mathbb{Z} \simeq ([0,1), \oplus) \simeq (S', \cdot) = \{z = \mathbb{C} : |z| = 1\}$

proof: let $f: \mathbb{R} \to [0,1)$ given by $f(a) = a \pmod 1$

$f(a+b) = f(a) \oplus f(b)$, so $f: \mathbb{R} \xrightarrow{\text{Hom}} [0,1)$, $\mathrm{Im}(f) = [0,1)$, $\ker(f) = \mathbb{Z}$

so $\mathbb{R}/\mathbb{Z} \simeq ([0,1), \oplus)$

Let $g: \mathbb{R} \to S'$ given by $g(a) = e^{2\pi i a}$

$g(a+b) = e^{2\pi i(a+b)} = e^{2\pi i a} \cdot e^{2\pi i b} = g(a) \cdot g(b)$, so $g: \mathbb{R} \xrightarrow{\text{Hom}} S'$

$\mathrm{Im}(g) = S'$, $\ker(g) = \mathbb{Z}$, so $\mathbb{R}/\mathbb{Z} \simeq (S', \cdot)$

Chapter 2

Ring Theory

Ex. ($\mathbb{Z}$ is not a group)

$2^{-1}=\frac{1}{2}\notin\mathbb{Z}$

Def. $(M,\cdot)$ monoid $\Leftrightarrow$

① "$\cdot$" binary operation

② $\forall\, a,b,c\in M,\ a(bc)=(ab)c$

③ $\exists\, 1\in M,\ \forall a\in M\ 1\cdot a=a\cdot 1=a$

Def. $(R,+,\cdot)$ is a ring $\Leftrightarrow$

① $(R,+)$ is an Abelian group

② $(R,\cdot)$ monoid

③ $\forall a,b,c\in R,\ a\cdot(b+c)=a\cdot b+a\cdot c$

④ If $(R,+,\cdot)$ is a commute ring, then $(R,\cdot)$ is Abelian

Thm. $(\mathbb{Z},+,\cdot),(\mathbb{Q},+,\cdot),(\mathbb{R},+,\cdot)\ (\mathbb{C},+,\cdot)$ are commute rings

Thm. $(\mathbb{R}^{n\times n},+,\cdot)$ is a non-commute ring

proof: $AB\neq BA$ in some cased

Thm. if $(R,+,\cdot)$ is a ring, then $\forall a\in R,\ 0\cdot a=0$

proof: $0=a-a=(1-1)a=0\cdot a$

Def. if $(R,+,\cdot)$ is a ring, define: $a-b=a+(-b)$

Thm. if $(R,+,\cdot)$ is a ring. $a,b\in R$, then $(-a)\cdot b=-(a\cdot b)=a\cdot(-b)$

Thm. if $(R,+,\cdot)$ is a ring, $a,b,c,d\in R$

then $(a+b)(c+d)=ac+ad+bc+bd$

Ex. if $(R,+,\cdot)$ is a ring
$a,b\in R$, $m,n\in\mathbb{Z}$
$ma\cdot nb=mn\,a\cdot b$

(Generalization of multiplication theorem)

Thm. if $(R,+,\cdot)$ is a commute ring, then

Binomial $(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$

Multinomial $(a_1+\cdots+a_m)^n=\sum_{k_1+\cdots+k_m=n}\binom{n}{k_1\cdots k_m}a_1^{k_1}\cdots a_m^{k_m}$

$\binom{n}{k}=C_n^k$ $\binom{n}{k_1\cdots k_m}=\frac{n!}{k_1!\cdots k_m!}$

proof: ② If $m=2$, $(a_1+a_2)^n=\sum_{k_1+k_2=n}\frac{n!}{k_1!k_2!}a_1^{k_1}a_2^{k_2}$

Apply induction on m, assume it holds for $m\le p-1$

when $m=p$ $(a_1+\cdots+a_{p-1}+a_p)^n=\sum_{k+k_p=n}\binom{n}{kk_p}(a_1+\cdots+a_{p-1})^k a_p^{k_p}$

$=\sum_{k+k_p=n}\sum_{k_1+\cdots+k_{p-1}=k}\binom{n}{kk_p}\binom{k}{k_1\cdots k_{p-1}}a_1^{k_1}\cdots a_{p-1}^{k_{p-1}}a_p^{k_p}$

$=\sum_{k+k_p=n}\sum_{k_1+\cdots+k_{p-1}=k}\binom{n}{k_1\cdots k_{p-1}k_p}a_1^{k_1}\cdots a_{p-1}^{k_{p-1}}a_p^{k_p}=\sum_{k_1+\cdots+k_p=n}\binom{n}{k_1\cdots k_p}a_1^{k_1}\cdots a_p^{k_p}$

so it holds for $\forall\, m\in\mathbb{N}^*$

Def. $(R,+,\cdot)$ is a ring, $a\in R$, $n\in\mathbb{N}^*$, then

$$\begin{cases} na=\underbrace{a+\cdots a}_{n} \\ 0a=0 \\ (-na)=(-n)a \end{cases}$$

Thm. $(R,+,\cdot)$ is a ring, $a,b\in R$, $n\in\mathbb{Z}$, then

$(na)\cdot b=n(a\cdot b)=a\cdot(nb)$

the proof is trivial

Thm. if $(R,+,\cdot)$ is a ring, $a\in R$, then

$(a+n1)(a-n1)=a^2-n^2 1$

Cor. $(A+nI)(A-nI)=A^2-n^2I$

Def. if $(R,+,\cdot)$ is a ring, then p is a polynomial with coefficients in $R \Leftrightarrow p(x)=a_0+a_1x+\cdots+a_nx^n=\sum_{i=0}^{n}a_ix^i$

Thm. p is a polynomial with coefficients in $R \Leftrightarrow$ $p(x)=\sum_{n=0}^{\infty}a_nx^n$, $\{a_n\}\subset R$, there are finite non-zero terms in $\{a_n\}$

Def. $\max\{n\in\mathbb{N}^*, a_n\neq 0\}=\deg p$

Def. if $(R,+,\cdot)$ is a ring, then

$R[x]=\{$polynomial with coefficients in $R\}$

$=\{p(x)=\sum_{n=0}^{\infty}a_nx^n : \{a_n\}\subset R$, with finite non-zero terms$\}$

Def. if $p,q\in R[x]$, $p(x)=\sum_n a_nx^n$, $q(x)=\sum_n b_nx^n$

Def. $p+q\in R[x]$ is given by $(p+q)x=\sum_n (a_n+b_n)x^n$

Def. $p\cdot q\in R[x]$ is given by $p(x)\cdot q(x)=(\sum_{n=0}^{\infty}a_nx^n)(\sum_{n=0}^{\infty}b_nx^n)$

$=\sum_{n=0}^{\infty}\sum_{k_1+k_2=n}(a_{k_1}\cdot b_{k_2})x^n$

Check that $\{a_n\}\cdot\{b_n\}\subset R$

all but finite $a_n+b_n=0$

$\sum_{k_1+k_2=n}a_{k_1}\cdot b_{k_2}\in R$

all but finite $\sum_{k_1+k_2=n}a_{k_1}\cdot b_{k_2}=0$

Thm. if $(R,+,\cdot)$ is a ring, then $(R[x],+,\cdot)$ is a ring.

proof: ① $\forall p,q\in R[x]$, $p+q\in R[x]$, $pq\in R[x]$,

② $p+q=\sum_n(a_n+b_n)x^n=\sum_n(b_n+a_n)x^n=q+p$

③ $p+0=0+p$, $p+q=q+p$, $pq=qp$

$\Rightarrow (R,+)$ is Abelian group

④ let $r\in R[x]$, $p(x)[q(x)r(x)]=(\sum_{n=0}^{\infty}a_nx^n)(\sum_{n=0}^{\infty}(\sum_{k_2+k_3=n}(b_{k_2}\cdot c_{k_3})x^n)$

$=\sum_{n=0}^{\infty}(\sum_{k_1+k=n}a_{k_1}(\sum_{k_2+k_3=k}(b_{k_2}\cdot c_{k_3})))x^n=\sum_{n=0}^{\infty}(\sum_{k_1+k_2+k_3=n}(a_{k_1}b_{k_2}c_{k_3}))x^n=[p(x)q(x)]r(x)$

so $(R[x],+,\cdot)$ is a ring

Ex. if $(R,+,\cdot)$ is a ring.
$\forall n\in\mathbb{Z}$, $n=n\cdot 1$, then
$(x+2y+3z+2y^2z^3+6x^2)(5x+30xy+7y^2)$
$=$

Def. $R[x_1,\cdots,x_n]=\left\{\sum_n\sum_{|\alpha|=n}a_\alpha x^\alpha : \{a_\alpha\}\subset R,\ x=(x_1,\cdots,x_n),\ \text{all but fin. } a_\alpha=0\right\}$

multi-index → $\alpha=(\alpha_1,\cdots,\alpha_n)$, $|\alpha|=\alpha_1+\cdots+\alpha_n$, $\alpha_i\in\mathbb{N}$

$x=(x_1,\cdots,x_n)$, $x^\alpha=x_1^{\alpha_1}\cdots x_n^{\alpha_n}$

Similarly

Def. $\sum_n\sum_{|\alpha|=n}a_\alpha x^\alpha+\sum_n\sum_{|\alpha|=n}b_\alpha x^\alpha=\sum_n\sum_{|\alpha|=n}(a_\alpha+b_\alpha)x^\alpha$

Def. $\left(\sum_n\sum_{|\alpha|=n}a_\alpha x^\alpha\right)\left(\sum_n\sum_{|\beta|=n}b_\beta x^\beta\right)=\sum_n\sum_{|\alpha|=n}\sum_{|\beta|+|\gamma|=|\alpha|}a_\beta b_\gamma x^\alpha$

* Prove that: if $(R,+,\cdot)$ is a ring, then $(R[x_1,\cdots,x_n],+,\cdot)$ is a ring

****Def.** if $(R,+,\cdot)$ is a ring, then
$S<R \iff S$ is a subring of R
$\iff$ ① $S\subset R$
② $(S,+,\cdot)$ is a ring

Thm. if $(R,+,\cdot)$ is a ring, then $S<R \iff$
① $S\subset R$, ① S is closed under "$+$", "$\cdot$"
② $0,1\in S$
③ $\forall a\in S$, $(-a)\in S$

Recall. $f: S\xrightarrow{\text{Hom}}S' \iff f$ preserves algebratic structure
For groups, in order to preserve { multiplication, identity element, inverse element }

Ex. $R[x_1,\cdots,x_m]<R[x_1,\cdots,x_p]$ $(m\le p)$

proof: $p(x)=\sum_n\sum_{|\alpha|=n}a_\alpha x^\alpha\in R[x_1,\cdots,x_m]$

$=\sum_n\sum_{k_1+\cdots+k_m=n}a_{k_1,\cdots,k_m}x_1^{k_1}\cdots x_m^{k_m}$

$=\sum_n\sum_{\substack{k_1+\cdots+k_m=n\\ k_{m+1}+\cdots+k_p=0}}a_{k_1,\cdots,k_m,\cdots,k_p}x_1^{k_1}\cdots x_m^{k_m}\cdots x_p^{k_p}\in R[x_1,\cdots,x_p]$

so $R[x_1,\cdots,x_m]\subset R[x_1,\cdots,x_p]$
Since they are both rings, then
$R[x_1,\cdots,x_m]<R[x_1,\cdots,x_p]$ $(m\le p)$

Def. if $(R,+,\cdot)$, $(R',+,\cdot)$

then $f: R \xrightarrow{\text{Hom}} R'$ Rings Homomorphism

$\Leftrightarrow \begin{cases} f(a+b)=f(a)+f(b) \\ f(ab)=f(a)f(b) \\ f(1)=1' \end{cases}$

Thm. if $(R,+,\cdot)$ is a ring. Fix $a\in R$, then

$\varphi: R[x] \xrightarrow{\text{Hom}} R$ is given by $\varphi(p)=p(a)$

i.e. $\varphi(\sum_n a_n x^n)=\sum_n a_n a^n$

proof: $\varphi(1)=1$, $\varphi(\sum_n a_n x^n+\sum_n b_n x^n)=\varphi(\sum_n (a_n+b_n)x^n)=\sum_n (a_n+b_n)a^n=\varphi(p)+\varphi(q)$

$\varphi\left((\sum_n a_n x^n)(\sum_n b_n x^n)\right)=\varphi(\sum_n(\sum_{k_1+k_2=n} a_{k_1}b_{k_2})x^n)=(\sum_n a_n a^n)(\sum_n b_n a^n)=\varphi(p)\varphi(q)$

Thm. if $(R,+,\cdot)$ is a ring, Fix $a=(a_1,\cdots,a_m)\in R^m$

Then $\varphi: R[x_1,\cdots,x_m] \xrightarrow{\text{Hom}} R$ is given by $\varphi(p)=p(a)$

i.e. $\varphi(\sum_n\sum_{|\alpha|=n} a_\alpha x^\alpha)=\sum_n\sum_{|\alpha|=n} a_\alpha a^\alpha$

proof: $\varphi(p+q)=\varphi(\sum_n\sum_{|\alpha|=n}(a_\alpha+b_\alpha)a^\alpha)=\sum_n\sum_{|\alpha|=n}(a_\alpha+b_\alpha)a^\alpha$

$=\sum_n\sum_{|\alpha|=n} a_\alpha a^\alpha+\sum_n\sum_{|\alpha|=n} b_\alpha a^\alpha=\varphi(p)+\varphi(q)$

$\varphi(pq)=\varphi\left(\sum_n\sum_{|\alpha|=n}\left(\sum_{|\beta|+|\gamma|=|\alpha|} a_\beta\cdot b_\gamma\right)x^\alpha\right)=\sum_n\sum_{|\alpha|=n}\left(\sum_{|\beta|+|\gamma|=|\alpha|} a_\beta b_\gamma\right)a^\alpha$

$=\left(\sum_n\sum_{|\alpha|=n} a_\alpha a^\alpha\right)\left(\sum_n\sum_{|\alpha|=n} b_\alpha a^\alpha\right)=\varphi(p)\varphi(q)$

Also, $\varphi(1)=1$, so $\varphi: R[x_1,\cdots,x_m] \xrightarrow{\text{Hom}} R$

Recall. $N\lhd G \Leftrightarrow N<G$ & $\forall\, a\in N$, $aN=Na$

$aN=\{ah, h\in N\}$, $Na=\{ha, h\in N\}$

"Def." if $(R,+,\cdot)$ is a ring, then I is an left ideal of $R \Leftrightarrow I$ allows $(R/I,+,\cdot)$ to be a ring

Def. $R/I = \{a+I : a \in R\}$

if we want $(R/I,+)$ to be an Abelian group, then we want $(I,+)$ to be a normal subgroup of $(R,+)$

i.e. $(I,+) < (R,+)$

Therefore, $(a+I)+(b+I) = (a+b)+(I+I) = (a+b)+I$

However, $(a+I)(b+I) = ab+(a+b)I+I$, thus we need $aI \subset I$

Def. if $(R,+,\cdot)$ is a ring, then $I \lhd R \Leftrightarrow$

I is an ideal of $R \Leftrightarrow$ ① $(I,+) < (R,+)$

② $\forall a \in R, aI \subset I$

(i.e. $\forall a \in R, \forall x \in I, ax \in I$)

Thm. if $I \lhd R$, then $(R/I,+,\cdot)$ is a ring.

proof: $R/I = \{a+I : a \in R\}$

$\forall a,b \in R, x,y \in I, (a+x)+(b+y) = (a+b)+(x+y)$

$(a+x)(b+y) = ab+ay+xb+xy = ab+ay+bx+xy$

$(a+I)((b+I)(c+I)) = ((a+I)(b+I))(c+I)$

$(1+I)(a+I) = (a+I)(1+I) = a+I$

$(a+I)((b+I)+(c+I)) = (a+I)(b+I)+(a+I)(c+I)$

Therefore $(R/I,+,\cdot)$ is a ring

Ex1. $(n\mathbb{Z},+,\cdot)\lhd(\mathbb{Z},+,\cdot)$

proof: ① $a=nk_1$, $b=nk_2$

$\Rightarrow a+b=n(k_1+k_2)\in n\mathbb{Z}$

② $\forall r\in\mathbb{Z}$, $x=nk$

$rx=rnk=n(rk)\in\mathbb{Z}$

Ex2. if $(R,+,\cdot)$ is a ring

Fix $a\in R$, Then $(a)=Ra\lhd R$

proof: ① $r_1a+r_2a=(r_1+r_2)a$

② if $r\in R$, $x\in(a)=Ra$

$x=r'a$,

$rx=(rr')a\in Ra$

so $Ra\lhd R$

Ex3. if $(R,+,\cdot)$ is a ring

Fix $a_1,\cdots,a_n\in R$, then

$(a_1,\cdots,a_n):=\{r_1a_1+\cdots+r_na_n : r_i\in R\}$

& $(a_1,\cdots,a_n)\lhd R$

proof: let $a,b\in(a_1,\cdots,a_n)$

$a=r_1a_1+\cdots+r_na_n$

$b=r_1'a_1+\cdots+r_n'a_n$

$a+b=(r_1+r_1')a_1+\cdots+(r_n+r_n')a_n\in(a_1,\cdots,a_n)$

let $r\in R$, $a\in(a_1,\cdots,a_n)$

then $ra=(rr_1)a_1+\cdots+(rr_n)a_n\in(a_1,\cdots,a_n)$

so $(a_1,\cdots,a_n)\lhd R$

More generally, Fix $v_1,\cdots,v_n\in V$

$F=\mathbb{R}$ or $\mathbb{C}$, then we have

$\operatorname{span}(v_1,\cdots,v_n)\lhd V$

Thm. $I\lhd R$ & $I<R \Leftrightarrow I=R$

proof: "<=" ✓

"=>": $(I,+)<(R,+)$, $\forall a\in R$, $aI\subset I$, while $(I,+,\cdot)$ is a ring

$(a+I)\cdot I=aI+I\subset I$, then for $\forall a\in R$, $x,y\in I$

$(a+x)\cdot y\in I$, then $(a+0)\cdot 1=a\in I$ for $\forall a\in R$

so $R\subset I$, Since $I\subset R$, therefore $I=R$

Thm. $I\lhd R \Leftrightarrow$ { ① $I\neq\emptyset$ ② $\forall r\in R, \forall x\in I, rx\in I$

proof: "=>" ✓

"<=" if I is closed under "+"

& $\forall a\in R, \forall x\in I, ax\in I$

WTS: $(I,+)<(R,+)$

Check: $0\in I$, let $x\in I$, $0\in R$, then $0\cdot x=0\in I$

Check: if $a\in I$, $-1\in R$, then $-1\cdot a=(-a)\in I$

Conclusion. To show $I\lhd R$, only show that

($①\ I\neq\emptyset$) { ① $\forall a,b\in I$, $a+b\in I$ ② $\forall r\in R, \forall x\in I$, $rx\in I$

Cor. $R\lhd R$

Thm. if $f: R \xrightarrow{Hom} R'$, then $Ker(f) \lhd R$, $Im(f) < R'$

proof: ① Check that $Ker(f) \lhd R$

Notice that $(Ker(f), +) < (R, +)$

while $\forall r \in R, x \in Ker(f)$, $f(rx) = f(r)f(x) = f(r) \cdot 0 = 0$

so $Ker(f) \lhd R$

② Check that $Im(f) < R'$, Clearly $Im(f) \subset R'$

$\forall a, b \in R$, $f(a) + f(b) = f(a+b) \in Im(f)$

$f(a) + f(b) = f(a+b) = f(b+a) = f(b) + f(a)$

$f(a) + f(0) = f(a) + f(0) = f(a)$

$f(a)f(1) = f(1)f(a) = f(a)$

$f(a) + f(-a) = f(0) = f(-a) + f(a)$

so $(Im(f), +, \cdot)$ is a ring, therefore $Im(f) < R'$

Cor. ① $(R/ker(f), +, \cdot)$ is a quotient ring

② $Im(f)$ is a ring

Def. $f: R \xrightarrow{Iso} R' <=>$ ① f is bijective ② f is homomorphic ③ f^{-1} is homomorphic

Thm. $f: R \xrightarrow{Iso} R' <=>$ ① f is bijective ② f is homomorphic

proof: "=>" is trivial

"<=" $f(a+b) = f(a) + f(b) = a' + b'$, $f(ab) = f(a)f(b) = a'b'$

then $f^{-1}(a') = a$, $f^{-1}(b') = b$ $f^{-1}(a'+b') = f^{-1}(a') + f^{-1}(b')$ $f^{-1}(a'b') = f^{-1}(a')f^{-1}(b')$

also $f^{-1}(1') = 1$, $f(1) = 1'$

First Ring Isomorphic Theorem

Thm. if $f: R \xrightarrow{Hom} R'$, then $R/\ker(f) \simeq \mathrm{Im}(f)$

proof: from previous theorem, $\ker(f) \lhd R$

Let $\hat{f}: R/\ker(f) \to \mathrm{Im}(f)$ given by $\hat{f}(x+I) = f(x)$, let $I = \ker(f)$

$\hat{f}(a+I) + \hat{f}(b+I) = f(a) + f(b) = f(a+b) = \hat{f}((a+I)+(b+I))$

$\hat{f}((a+I)(b+I)) = \hat{f}(ab+(a+b)I+I) = \hat{f}(ab+I) = f(ab) = f(a)f(b)$

$= \hat{f}(a+I)\hat{f}(b+I)$

Reversely, let $\hat{f}^{-1}: \mathrm{Im}(f) \to R/I$ given by $\hat{f}^{-1}(a) = a+I$

$\hat{f}^{-1}(a+b) = (a+b)+I = (a+I)+(b+I) = \hat{f}^{-1}(a) + \hat{f}^{-1}(b)$

$\hat{f}^{-1}(ab) = ab+I = (a+I)(b+I) = \hat{f}^{-1}(a)\hat{f}^{-1}(b)$

so $\hat{f}: R/\ker(f) \xrightarrow{Iso} \mathrm{Im}(f)$, $\Leftrightarrow R/\ker(f) \simeq \mathrm{Im}(f)$

Def. if $(R, +, \cdot)$ is a ring, then $u \in R$ is a unit $\Leftrightarrow$ u has a multiplicational inverse $\Leftrightarrow \exists\, v \in R$, s.t. $u \cdot v = v \cdot u = 1$

Thm. - $(\mathbb{Z}, +, \cdot)$, u is a unit $\Leftrightarrow u = \pm 1$

Thm. p is a unit of $(R[x], \cdot, +) \Leftrightarrow p \equiv u$, u is a unit in $(R, \cdot, +)$

proof: "$\Leftarrow$" $p \equiv u$, then $\exists v$ s.t. $u \cdot v = v \cdot u = 1$

let $q \equiv v$ then $p \cdot q = q \cdot p = 1$

"$\Rightarrow$" $p(x) = \sum_n a_n x^n$, $\exists\, q$, s.t. $p \cdot q = q \cdot p = 1$

let $q = \sum_n b_n x^n$, then $p \cdot q = q \cdot p = \sum_n \sum_{k_1+k_2=n} (a_{k_1} b_{k_2}) x^n = 1$

Recall that $\deg(p) = \max\{n \in \mathbb{N} : a_n \neq 0\}$

$q \cdot p = p \cdot q = 1 \Leftrightarrow \deg(pq) = 0 \Rightarrow a_0 b_0 = b_0 a_0 = 1$

Since $p \equiv u$, then $\deg(p) = 0$, so $u \equiv a_0$, let $v \equiv b_0$

then $\exists v$, $uv = vu = 1$

Ex:
$(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ are fields

Def. $(F,+,\cdot)$ is a field $\Leftrightarrow$

① $(F,+)$ is an Abelian group

② $(F\setminus\{0\},\cdot)$ is an Abelian group

③ Distributivity, i.e. $\forall a,b\in F$, $a(b+c)=ab+ac$

Thm. if $(F,+,\cdot)$ is a field, then $(F,+,\cdot)$ is a ring.

proof: $(F,+)$ is an Abelian group

$\exists\, 1\in F$, s.t. $a\cdot 1=a$, $a+0=0+a$

Thm. if $(F,+,\cdot)$ is a field, then u is a unit in F

$\Leftrightarrow u\neq 0$

proof: ① if $u\neq 0$, $\exists u^{-1}$ s.t. $uu^{-1}=u^{-1}u=1$

② if $u=0$, $uv=vu=0\neq 1$, so $u\neq 0$

Cor. if $(F,+,\cdot)$ is a field, then P is a unit in $(F[x],+,\cdot)$

$\Leftrightarrow P\equiv u$, $u\in F^{\times}$

Def. if $(R,+,\cdot)$ is a ring, $a\in R$, then

a is a left/right divisor $\Leftrightarrow \exists\, b\in R$ s.t. $ab=0$ / $ba=0$

Ex.

$\mathbb{Z}_6$ is not a integral ring

$\bar{2}\cdot\bar{3}=\bar{0}$

so 0 is not the only divisor

Def. $(R,+,\cdot)$ is an integral domain (entire ring) 整环

$\Leftrightarrow$ { ① $0\neq 1$ (R is not a zero ring)

② the only zero divisor is 0

③ R is communicative, i.e. $ab=ba$

Prop. if $(R,+,\cdot)$ is an integral domain & $ab=ac$, $a\neq 0$

then $b=c$

Thm. $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ are integral domains.

Ex.

$\mathbb{Z}_6$ is not a integral ri

$\bar{2}\cdot\bar{3}=\bar{0}$

so 0 is not the only divisor

Ex. ① $10\in\mathbb{Z}$ is reducible since $10=2\cdot5$

② $x^2-2x-3\in\mathbb{Z}[x]$ is reducible $(x^2-2x-3)=(x-3)(x+1)$

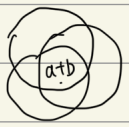
③ if $p\in\mathcal{P}$ (prime), then $p\in\mathbb{Z}$ is not reducible

Def. if $(R,+,\cdot)$ is a ring, $a\in R\setminus\{0\}$, then

- a is reducible $\Leftrightarrow \exists\, b,c$ non-unit, s.t. $a=bc$
- a is irreducible $\Leftrightarrow \forall\, b,c$ non-unit, $a\neq bc$

.

Recall that. $I\lhd R \Leftrightarrow$
- $\forall a,b\in I,\ a+b\in I$
- $\forall r\in R, \forall a\in I,\ ra\in I$



Thm. if $\forall \alpha\in I$, $I_\alpha\lhd R$, then $\bigcap_{\alpha\in I} I_\alpha \lhd R$

(Here I_α is the set that contains α)

proof: Check.1 if $a,b\in\bigcap_{\alpha\in I} I_\alpha$, then $a+b\in\bigcap_{\alpha\in I} I_\alpha\lhd R$

$\forall\alpha\in I$, $\forall a,b\in I_\alpha$, $\Rightarrow \forall\alpha\in I$, $a+b\in I_\alpha$

By the arbitariness of I_α, $a,b\in\bigcup_{\alpha\in I} I_\alpha \Rightarrow a+b\in\bigcup_{\alpha\in I} I_\alpha$

Check.2 if $r\in R$, $a\in\bigcap_{\alpha\in I} I_\alpha$, then $ra\in\bigcap_{\alpha\in I} I_\alpha$

Let $r\in R$, $a\in\bigcap_{\alpha\in I} I_\alpha$

$\forall\alpha\in I$, $a\in I_\alpha$, $I_\alpha\lhd R \Rightarrow \forall\alpha\in I$, $ra\in I_\alpha$

so $ra\in\bigcap_{\alpha\in I} I_\alpha$

Thm. if $I_1,\cdots,I_n\lhd R$, then $I_1+\cdots+I_n\lhd R$

Recall $I_1+\cdots+I_n=\{a_1+\cdots+a_n : a_i\in I_i\}$

Check.1 $a,b\in I_1+\cdots+I_n \Rightarrow a+b\in I_1+\cdots+I_n$

Let $a,b\in I_1+\cdots+I_n$, $a=a_1+\cdots+a_n$, $b=b_1+\cdots+b_n$

$a+b=(a_1+b_1)+\cdots+(a_n+b_n)\in I_1+\cdots+I_n$ (Since $(I_i,+)$ is Abelian)

Def: $(R,+,\cdot)$ is an integral domain (entire ring) 整环

$\Leftrightarrow$ ① $0 \neq 1$ (R is not a zero ring)

② the only zero divisor is 0

③ R is communicative, i.e. $ab=ba$

Ex. $(\mathbb{Z},+,\cdot)$ is a PID

proof: if $I \lhd \mathbb{Z}$ proper

then $(I,+) < (\mathbb{Z},+)$

if $I=\{0\}$, $I=(0)=R\cdot 0$ ✓

otherwise, $I \neq \{0\}$

let $m = \min\{\mathbb{N}^* \cap I\}$

Check 1. $I \supset m\mathbb{Z}$

$\forall a \in \mathbb{Z}$, $ma \in I$, so $m\mathbb{Z} \subset I$

Check 2. $I \subset m\mathbb{Z}$

suppose $\exists n \in I$, s.t. $n \notin m\mathbb{Z}$

i.e. $\gcd(m,n)=1$

if $m=1$, then $I \subset \mathbb{Z}$ ✓

otherwise, since $\gcd(m,n)=1$

then $\exists r \in \mathbb{Z}$, s.t. $m+rn \notin I$

which contradicts

so $I \subset m\mathbb{Z}$

Therefore, $\forall I \lhd \mathbb{Z}$, $\exists m \in \mathbb{Z}$, $I=m\mathbb{Z}$

Since $\mathbb{Z}$ is communicative, $I=\mathbb{Z}m$

so $(\mathbb{Z},+,\cdot)$ is a PID

Recall. $I \lhd R \Leftrightarrow I$ is a principle ideal $\Leftrightarrow \exists a \in R$, s.t. $I=(a)=Ra$

Def. $(R,+,\cdot)$ is a PID (principle ideal domain) $\Leftrightarrow$

① $(R,+,\cdot)$ is an intergral domain

② $\forall I \lhd R$ proper, I is principle

($I \neq R$)

Recall. if $(R,+,\cdot)$ is a ring, then u is a unit of $R \Leftrightarrow$ $\exists v \in R$, s.t. $uv=vu=1$

Thm. if $(R,+,\cdot)$ is a ring, let $U=\{u \in R \text{ unit}\}$

then $(U,\cdot)$ is a group.

proof: ① $u_1, u_2 \in U$, $u_1v_1=v_1u_1=u_2v_2=v_2u_2=1$

then $u_1u_2v_2v_1=1$, i.e. $u_1u_2 \in U$

② $u \in R$, so $1\cdot u = u\cdot 1 = u$

③ $\forall u \in U$, $\exists v \in U$, s.t. $u\cdot v = v\cdot u = 1$, i.e. $v=u^{-1}$

④ $u,v,w \in U \subset R$, so $u(vw)=(uv)w$

Def. if $(R,+,\cdot)$ is an integral ring, $a \in R \setminus \{0\}$

then a has a unique factorization $\Leftrightarrow$

① if $a=up_1\cdots p_n = u'p_1'\cdots p_m'$

where u,u' unit, $p_1,\cdots,p_n,p_1',\cdots p_m'$ irreducible

then $m=n$ & $\exists \sigma \in S_n = \{\sigma : \{1,\cdots,n\} \xrightarrow{\text{bij}} \{1,\cdots,n\}\}$ s.t.

$\forall i \in \{1,\cdots,n\}$, $\exists u_i$ unit, s.t. $p'_{\sigma(i)} = u_i p_i$

(Since u has a multiplicative inverse, $p_i = u_i^{-1} p'_{\sigma(i)}$, where $u_i^{-1} \in U$)

($\Leftrightarrow \forall i$, $\exists v_i$, s.t. $p_{\sigma(i)} = v_i p_i'$)

② $\exists$ unique u unit, $\exists p_1,\cdots,p_n$ irreducible, s.t.

$a=up_1\cdots p_n$

Ex.
$(\mathbb{Z},+,\cdot)$ is a UFD

Def. if $(R,+,\cdot)$ is a ring, then $(R,+,\cdot)$ is a UFD unique factorization domain $\Leftrightarrow$

① $(R,+,\cdot)$ is an integral domain

② $\forall a\in R/\{0\}$, $\exists$ unique factorization

Thm. (Fundamental Theorem of Arithnetic) (FTA)

$\forall n\in\mathbb{N}_1, \exists! m\in\mathbb{N}_1, \exists! p_1<\cdots<p_m\in\mathbb{P}, \exists! s_1,\cdots,s_m\in\mathbb{N}$, s.t.

$n=p_1^{s_1}\cdots p_m^{s_m}$

Cor: $(\mathbb{Z},+,\cdot)$ is a UFD

Lemma. $p\in\mathbb{Z}\setminus\{0\}$ irreducible $\Leftrightarrow |p|\in\mathbb{P}$

(pf) p is irreducible $\Leftrightarrow \forall b,c\neq\pm1$, $p\neq bc$

$\Leftrightarrow \forall b,c\in\mathbb{N}_1$, $|p|\neq bc$ $\Leftrightarrow |p|\in\mathbb{P}$

Check1. $\mathbb{Z}$ is an integral domain ✓

Check2. $\forall a\in\mathbb{Z}\setminus\{0\}$, a has unique factorization

By FDA, $|a|=p_1^{s_1}\cdots p_m^{s_m}$, then $a=(-1)^r p_1^{s_1}\cdots p_m^{s_m}$, wher $r\in\mathbb{N}^*$

notice that $\{1,-1\}$ is the set of all units of $\mathbb{Z}$

Since $p_i\in\mathbb{P}$, then p_i is irreducible

$a=(-1)^r\cdot\overbrace{p_1\cdots p_1}^{s_1}\cdots\overbrace{p_m\cdots p_m}^{s_m}$, which is

Goal 1. if $(R,+,\cdot)$ is a PID, then it is a UFD

Def: If $(R,+,\cdot)$ is an integral domain, then

$a|b \Leftrightarrow \exists c \in R$, s.t. $b=ac$

Thm. Assume $(R,+,\cdot)$ integral domain (up to a unit)

define $a \sim b \Leftrightarrow \exists u \in U$, s.t. $a=ub$.

Then "$\sim$" is a equivallent relation

proof: if $a \sim b$, $b \sim c$, then $a=u_1 b = u_1 u_2 c$

Since U is a group, then $u_1 u_2 \in U$, so $a \sim c$

$a = 1 \cdot a$, so $a \sim a$

$\exists v$, s.t. $uv=vu=1$, then $va = vub = b$, so $a \sim b \Leftrightarrow b \sim a$

Thm. if $(R,+,\cdot)$ is an integral domain, then "$|$" is preorder (原序) (i.e. reflexive & transive)

proof: $\forall a \in R$, $a \cdot 1 = a$, so $a|a$

if $a|b$, $b|c$, then $\exists e, f \in R$, $b=ae$, $c=bf$

so $c = aef = a(ef)$ $\surd$

Thm. if $(R,+,\cdot)$ is an integral domain, then $a \sim b$ $\Leftrightarrow a|b$ & $b|a$

proof: $a|b$ & $b|a \Rightarrow \exists u, v \in R$, s.t. $b=au$, $a=bv$

so $b = buv \Rightarrow b \cdot 1 = b \cdot uv$, since R is an integral domain

then $uv = vu = 1$, i.e. v, u are unit, therefore $a \sim b$

$a \sim b \Rightarrow \exists u$ unit, $a=ub$, thus $\exists v$, s.t. $b=av$

i.e. $a|b$ & $b|a$

Ex. if $(R,+,\cdot)$ is an integral domain, $u\in U$, $a\in R$ then $u|a$

pf:) $u\in U$, then $\exists v\in U$, $uv=vu=1$

$a=(uv)a=u(va)$, so $u|a$

$\mathbb{Z}$ is a PID

① if $I=\{0\}$, then $I=0\mathbb{Z}$ ✓

② if $I\neq\{0\}$, take $b\in I\setminus\{0\}$, where $\forall x\in I\setminus\{0\}$, $|b|\leq|x|$

Claim. $I=(b)$

$\forall z\in\mathbb{Z}$, $zb\in I$

Suppose $\exists c\in I\setminus(b)$

then $c=qb+r$, $r\in I$

However $|r|<|b|$ ⚡

Def. if $(R,+,\cdot)$ is an integral domain, $p\in R\setminus\{0\}$ then p is prime $\Leftrightarrow(p|ab\Rightarrow p|a$ or $p|b)$

Note that p is prime $\Rightarrow$ irreducible

irreducible $\not\Rightarrow$ prime, it holds only if R is UFD

Prop. p is prime $\Leftrightarrow(p|a\Rightarrow p\sim a)$

Thm. if $(R,+,\cdot)$ is an integral domain, p is prime, then p is irreducible.

proof: if p is reducible, then $\exists\, a,b$ non-unit, $p=ab$

clearly $p|ab$, however if $p|a$, then $\exists c$, s.t. $a=pc$

this contradicts since b is non-unit, so p is not prime

Assume p is prime, WLOG $p|a$, then $a=pc$ where $c\in R$

So $p=ab=p(cb)$, $\Rightarrow cb=1$

So every prime element is irreducible in integral domain.

Thm. if $(R,+,\cdot)$ is a UFD, p irreducible, then p is prime

proof: Assume $(R,+,\cdot)$ UFD & $p\in R\setminus\{0\}$ irreducible

WTS: if $p|ab$, then $p|a$ or $p|b$

Assume $p|ab$, then $\exists\, d\in R$, $ab=pd$, $d\in R$

$a=up_1\cdots p_m$, $u\in U$, p_i irreducible

$b=vq_1\cdots q_n$, $v\in U$, q_i irreducible

$d=wr_1\cdots r_l$, $r\in U$, r_i irreducible

then $wr_1\cdots r_l p=uvp_1\cdots p_m q_1\cdots q_n$, thus $pr_1\cdots r_l\sim p_1\cdots p_m q_1\cdots q_n$

since factorization is unique, the $l+1=m+n$

then $\exists i$, s.t. $p\sim p_i$ or $p\sim q_i$ thus $\exists s\in U$, $q_i=ps$ or $p_i=ps$

so $p|a$ or $p|b$, therefore p is prime

Lemma. if $p\sim p_i$, $p_i|a$, then $p|a$

proof: $\exists u\in U$, $p_i=up$

$\exists c\in R$, $a=cp_i=(cu)p$

therefore

Lemma. if p,q are prime, then $p|q$ & $q|p\Rightarrow p\sim q$

proof: $\exists c\in R$, $q=cp$, $\exists d\in R$, $p=dq$, thus $q=(cd)q$

Since $(R,+,\cdot)$ is integral domain, then $cd=1$, i.e. $c,d\in U$

Hence $p\sim q$

Thm. if $(R,+,\cdot)$ is an integral domain, then $(R,+,\cdot)$ UFD $\Leftrightarrow$ Every irreducible element is a prime & Every $a\in R\setminus\{0\}$ has a factorization

proof: "$\Rightarrow$" $\surd$

"$\Leftarrow$": Assume $a\in R\setminus\{0\}$, then $\exists u\in U$, $a=up_1\cdots p_m$ where $p_1,\cdots p_m$ are irreducible and prime

Assume $\exists\, v\in U$, $a=vq_1\cdots q_m=up_1\cdots p_m$,

Notice that $p_i \mid vq_1\cdots q_n$, $q_1\cdots q_m\sim vq_1\cdots q_n$

therefore $p_i\mid q_1\cdots q_n$, thus $\exists$ some unique j, s.t. $p_i\mid q_j$

conversely, $\exists$ some i, s.t. $q_j\mid p_i$

Hence $m=n$, $p_i\sim q_j$ for some i,j

Thus $\exists\,\sigma:\{1,\cdots,n\}\xrightarrow{bij}\{1,\cdots,n\}$, s.t. $\sigma(i)=j$

let $q_j=v_jp_j'=v_jp'_{\sigma(i)}$, $w=vv_1\cdots v_n$, hence $a=wp'_{\sigma(1)}\cdots p'_{\sigma(n)}=up_1\cdots p_n$

Therefore any factorization is unique, R is a UFD

Def. if $(R,+,\cdot)$ is an integral domain, then $d=\gcd(a,b)$ $\Leftrightarrow$ (greatest common divisor)

① $d\mid a$ & $d\mid b$

② if $e\mid a$ & $e\mid b$, then $e\mid d$

Lemma. $\gcd(a,b)$ is unique up to a unit

i.e. if $d=\gcd(a,b)$, $e=\gcd(a,b)$, then $d\sim e$

proof: Since $e\mid a$ & $e\mid b$, then $e\mid d$

Similarly, we have $d\mid e$, thus $e\sim d$

$I \lhd R \iff \begin{cases} (I,+) < (R,+) \\ \forall a \in R,\ aI \subset I \end{cases}$

Def. if R I.D., then $m = lcm(a,b) \iff$ (least common multiplier)

① $a|m$ & $b|m$

② if $a|n$ & $b|n$, then $m|n$

$(R,+,\cdot)$ PID $\iff$

$\begin{cases} ① (R,+,\cdot) \text{ is integral domain} \\ ② \forall I \lhd R, I \text{ is proper} \end{cases}$

Thm. if $(R,+,\cdot)$ PID, then $\forall a,b \in R, \exists d \in R$, s.t. $(a)+(b)=(d)$ & $d=gcd(a,b)$

proof: Since $(R,+,\cdot)$ PID, $(a) \lhd R$, $(b) \lhd R$, then $(a)+(b) \lhd R$

thus $\exists d \in R$, $(a)+(b)=(d)$

if $(a)+(b) \neq R = (1)$, then $\overset{PID}{\Longrightarrow} \exists d \in R$, s.t.

$(d) = (a)+(b) = \{ma+nb : m,n \in R\} = \{dr : r \in R\}$

WTS 1. $d|a$ & $d|b$

$\{0\} \subset (a)$, $\{0\} \subset (b)$

So $(a) \subset (a)+(b) = (d)$, $a = rd$ for some r, $d|a$

Similarly we have $d|b$

WTS 2. if $e|a$ & $e|b$, then $e|d$

we try to show that if $(b) \subset (e)$ & $(a) \subset (e)$, then $(d) \subset (e)$

$(d) = (a)+(b) \subset (e)+(e) = (e)$, thus $e|d$

so $d = gcd(a,b)$

if $(a)+(b) = (1)$, clearly $\forall r \in R \setminus \{0\}$, $1|r$, thus $gcd(a,b)=1$

Cor. if $a,b \in \mathbb{N}_1$, then $a\mathbb{Z}+b\mathbb{Z} = gcd(a,b)\mathbb{Z}$

Notice that $\mathbb{Z}$ is a PID, thus it holds

Cor. $a\mathbb{Z}+b\mathbb{Z} = \mathbb{Z} \Rightarrow gcd(a,b)=1$

if $a,b \in \mathbb{N}_1$, obviously it holds

if $a=1$, $\mathbb{Z} \subset \mathbb{Z}+b\mathbb{Z} \subset \mathbb{Z}$ ✓

Lemma.
$(d) \subset (a) \iff a \mid d$

proof: $\{dr : r \in R\} \subset \{ap : p \in R\}$
thus $d = ap$ for some $p \in R$, $a \mid d$
if $a \mid d$, $d = ap$ for some $p \in R$
then $\forall r \in R$, $rd = a(rp)$
Hence $(d) \subset (a)$

Thm. if $(R, +, \cdot)$ PID, then $\forall a, b \in R$, $\exists m \in R$
s.t. $(a) \cap (b) = (m)$ & $m = lcm(a, b)$

proof: $(a) \lhd I$, $b \lhd I$, thus $(a) \cap (b) \lhd I$

① if $(a) \cap (b) \neq R$, then $\overset{PID}{\Rightarrow} \exists m \in R$, s.t. $(a) \cap (b) = (m)$

Thus $(m) \subset (a)$ & $(m) \subset (b)$, so $a \mid m$ & $b \mid m$

if $a \mid n$ & $b \mid n$, then, $(n) \subset (a)$ & $(n) \subset (b)$

so $(n) \subset (a) \cap (b) = (m)$, hence $(n) \subset (m) \iff n \mid m$

so $m = lcm(a, b)$

② if $(a) \cap (b) = R$, Since $(a), (b) \subset R$, then $(a), (b) = R$

Thus, $a \sim b \sim 1$, $a \mid 1$ & $b \mid 1$ while $\forall e \in R$, $e \mid 1$

so $m = lcm(a, b) = 1$

Cor. if $a, b \in \mathbb{N}$, then $a\mathbb{Z} \cap b\mathbb{Z} = lcm(a, b)\mathbb{Z}$

Clearly $\mathbb{Z}$ is an intergral domain

Lemma. $gcd(a, b)\, lcm(a, b) \sim ab$ (From Elementry Number Theory)

proof: let $d = gcd(a, b)$, $m = lcm(a, b)$

$(d) = (a) + (b)$, $(m) = (a) \cap (b)$

$(ab) = \{abr : r \in R\}$

$((a) + (b)) \cdot (a) \cap (b) = \{pax + qbx : p, q \in R, x \in (a) \cap (b)\}$

$\forall r \in R$, $abr \in \{pax + qbx : p, q \in R, x \in (a) \cap (b)\}$

let $x = r_1 a = r_2 b$, where $r_2 = s(r_1)$, thus $\forall p, q, r_1 \in R$

$pas(r_1)b + qr_1 ab = (ps(r_1) + qr_1)ab \in (ab)$

Hence $(ab) = [(a) + (b)] \cdot (a) \cap (b) = (md)$

And therefore $ab \sim md$

i.e. $gcd(a, b) \cdot lcm(a, b) \sim ab$

Collary.

$a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z} \iff gcd(a, b) = 1$

$(a_1) \subsetneq (a_2) \subsetneq \cdots$

Lemma. if $(R,+,\cdot)$ PID & p irreducible, $p \nmid a$ then $\gcd(a,p)=1$

proof: Clearly $1 \mid a$ & $1 \mid p$ ✓

Check. if $d \mid a$ & $d \mid p$, then $d \mid 1 \Leftrightarrow d \sim 1 \Leftrightarrow d \in U$

Assume $d \notin U$, $d \mid p \Rightarrow \exists e \in R$, $p = ed$

since p is irreducible, $d \notin U$, then $e \in U$

so $p \sim d$, from $d \mid a$, we have $p \mid a$, which contradicts $d \mid a$ & $d \mid p \Rightarrow d \mid 1$, therefore $\gcd(a,p)=1$

☆☆☆

Thm. if $(R,+,\cdot)$ PID, then $(R,+,\cdot)$ UFD

proof: Check1. Every irreducible element is prime.

suppose $p \nmid a$, p irreducible, $p \mid ab$

Then we have $\gcd(a,p)=1$, $\exists d,e \in R$, s.t. $da+ep=1$

Since $p \mid ab$, $\exists f \in R$ s.t. $pf=ab$

Then $dab+epb=b \Rightarrow pdf+epb=(df+eb)p=b$

thus $p \mid b$, i.e. p is prime

Check2 Every element in $R \setminus \{0\}$ has a factorization

Let $S = \{s \in R \setminus \{0\}$: s can't be factorized up to $up_1 \cdots p_n$ where $u \in U$ & $p_1, \cdots, p_n$ irreducible$\}$. WTS: $S = \emptyset$

Assume $S \neq \emptyset$. Let $a_1 \in S$, then $a_1 \notin U$, so $(a_1) \lhd R$

Claim. There are no infinite ascending chain of principal ideals

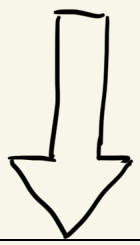
i.e. $\neg \exists \{a_n\}_{n \in \mathbb{N}} \subset S$, s.t. $(a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \subsetneq \cdots$

pf): Check. If so, then $\bigcup_n (a_n) \lhd R$

Check1: if $a, b \in \bigcup_n (a_n)$, then $a+b \in \bigcup_n (a_n)$

$\exists m,n \in \mathbb{N}$, s.t. $a \in (a_m)$, $b \in (a_n)$, and since $(a_{\min\{m,n\}}) \subsetneq (a_{\max\{m,n\}})$ then $a,b \in (a_{\max\{m,n\}})$, thus $a+b \in (a_{\max\{m,n\}}) \subset \bigcup_n (a_n)$

we continue on the next page



Check2. if $r \in R$, $a \in \bigcup_n (a_n)$, then $ra \in \bigcup_n (a_n)$

$\exists m \in \mathbb{N}$, s.t. $a \in (a_m)$, since $(a_m) \lhd R$, then

$ra \in (a_m) \subset \bigcup_n (a_n)$

Therefore, the ascending chain $\Rightarrow \bigcup_n (a_n) \lhd R$

Since $(R, +, \cdot)$ is a PID, then $\exists a \in R$, s.t. $\bigcup_n (a_n) = (a)$

$\exists m \in \mathbb{N}$, s.t. $a \in (a_m)$. Thus $(a) \subset (a_m) \Rightarrow \bigcup_n (a_n) \subset (a_m)$

$\Rightarrow \forall s \in \mathbb{N}, (a_{m+s}) = (a_m)$, which contradicts

Hence every ascending chain of principal ideals has an upper bound

& "$\subset$" is a partial order on the set of all principal ideals in R

By Zorn's Lemma, $\exists$ maximal ideal

Let $(a_1) \subsetneq \cdots \subsetneq (a_n)$ be a maximal ascending chain.

Case1. a_n irreducible

then $a_n = 1 \cdot a_n$, which is a factorization, contradicts

Case2. a_n reducible

then $a_n = bc$, where $b, c \notin U$, thus w.l.o.g. $b \in S$, $(a_n) \subset (b_n)$

However, (a_n) is the maximal ascending set, $(a_n) \subset (b) \Rightarrow a_n \sim b$

which contradicts with that $c \notin U$

Therefore, $(a_n) = \emptyset$, and thus $S = \emptyset$

And we are done:

PID $\Rightarrow$ UID $\Rightarrow$ integral domain

Recall
$R/I = \{a+I : a \in R\}$

$\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$

Notice that

$f: \mathbb{R}[x] \longrightarrow \mathbb{C}$ given by

$f(p) = p(i)$ is homomorphic

Since $f(\sum_n a_n x^n) + f(\sum_n b_n x^n)$

$= f(\sum_n a_n x^n + \sum_n b_n x^n)$

$f(p \cdot q) = f(p) \cdot f(q)$

$\ker(f) = (x^2+1)$

thus $\mathbb{R}[x]/(x^2+1) = \mathbb{C}$

Ex.

$\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$

proof: Clearly $\{a+bi : a,b \in \mathbb{Z}\} \subset \mathbb{Z}[i]$

$z = (a_0 - a_2 + a_4 \cdots) + (a_1 - a_3 + \cdots)i \in \{a+bi, a,b \in \mathbb{Z}\}$

thus $\mathbb{Z}[i] = \{a+bi : a,b \in \mathbb{Z}\}$

$(1, i)$ is a basis of $\mathbb{Z}[i]$

Ex. $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$

$\mathbb{Q}[\sqrt[3]{2}] = \{a+b\sqrt[3]{2}+c\sqrt[3]{4} : a,b,c \in \mathbb{Q}\}$

Since $\min\{n \in \mathbb{N} : (\sqrt[3]{2})^n \in \mathbb{Q}\} = 3$

$\Rightarrow (1, \sqrt[3]{2}, \sqrt[3]{4})$ is a basis for $\mathbb{Q}[\sqrt[3]{2}]$

$\mathbb{Q}[\pi] = \{a_0 + \cdots + a_n \pi^n + \cdots : a_0, \cdots \in \mathbb{Q}\}$

$(1, \pi, \cdots, \pi^n, \cdots)$ is a basis for $\mathbb{Q}[\pi]$

$\mathbb{Z}[\sqrt{-5}] = \{a+\sqrt{5}bi : a, b \in \mathbb{Z}\}$

Def. $\pi: R \to R/I$ is a collapse $\Leftrightarrow$
$I = (a_1, \cdots, a_n)$ where $a_1, \cdots, a_n \in R$

Def. if $R < S$, $s \in S \setminus R$, then $R[s]$ is the smallest ring containing both R & $\{s\}$ in S

Claim. $R[s] = \{r_0 + r_1 s + \cdots + r_n s^n, s \in S, r_0, \cdots, r_n \in R\}$

proof: Check. $R[s]$ is a ring

① $R[x] = \{p(x) = r_0 + \cdots + r_n x^n : r_0 \cdots r_n \in R\}$

② Let $f: R[x] \xrightarrow{\text{Hom}} S$ given by $f(p(x)) = p(s)$

Since $R < S$, $s \in S$, then $p(s) \in S$

And hence $\text{Im}(f) = R[s] < S$, $R[s]$ is a ring

Check. $R[s]$ is the smallest ring containing R & $\{s\}$

Suppose $R' \supset R \cup \{s\}$ is a ring

if R' is a ring, then $r_0 + r_1 s + \cdots + r_n s^n + \cdots \in R'$

Therefore $R[s] \subset R'$, thus $R[s]$ is the smallest ring.

Recall: $I \lhd R \Leftrightarrow (R/I, +, \cdot)$ is a ring

$(R, +, \cdot)$ PID $\Leftrightarrow \forall I \lhd R$, I is principal, $\exists a \in R$, s.t. $I = (a)$

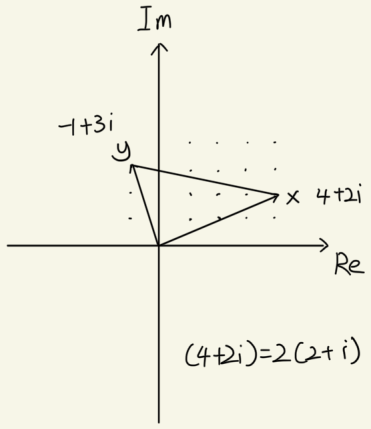
Division Algorithm

$\forall a \in \mathbb{Z}$, $\forall b \in \mathbb{Z} \setminus \{0\}$, $\exists! q, r \in \mathbb{Z}$, s.t.

$a = bq + r$, where $0 \le r < |b|$

Ex. $\mathbb{Z}[\sqrt{-5}]$ is not a UFD

proof: $6 = (1+\sqrt{5}i)(1-\sqrt{5}i) = 2 \times 3$ ※



Def. $(R,+,\cdot)$ is a Euclidian Domain $\Leftrightarrow$
$(R,+,\cdot)$ is an integral domain. $\exists f: R\setminus\{0\}\to\mathbb{N}$, s.t.
if $a,b\in R$, $b\neq 0$, $\exists q,r\in R$, s.t.
$a=bq+r$, where $r=0$ or $f(r)<f(b)$

Thm. A field is an Euclidian Domain

proof: Let $(R,+,\cdot)$ be a field
i.e. $(R\setminus\{0\},\cdot)$ & $(R,+)$ Abelian, $(R,+,\cdot)$ integral domain
Let $a,b\in R$, $b\neq 0$, if $a=0$, then $a=0\cdot b+0$ ✓
if $a\neq 0$, $a=(ab^{-1})b+0$, $r=0$ ✓
Clearly, the proof is done

Thm. A Euclidian Domain is a PID

proof: Let $(R,+,\cdot)$ be an Euclidian Domain
i.e. if $a,b\in R$, $b\neq 0$, then $\exists q,r\in R$, s.t. $a=bq+r$
where $r=0$ or $f(r)<f(b)$
Check: if $I\lhd R$ proper, then I is principal
If $I=\{0\}$, clearly $I=(0)$ ✓
Otherwise, $I\setminus\{0\}\neq\emptyset$. Consider $f: I\setminus\{0\}\to\mathbb{N}$
Clearly f is bounded below, Take $b=\underset{x\in I\setminus\{0\}}{\operatorname{argmin}} f(x)$
Claim. $I=(b)$, let $r\in R$, $b\in I$, so $rb\in I$, so $(b)\subset I$
Conversely, suppose $a\in I\setminus(b)$, $a=qb+r$, $r=0$ or $f(r)<f(b)$
① if $r=0$, $a=qb\in(b)$, which contradicts
② if $r\neq 0$, since $b=\underset{x\in I\setminus\{0\}}{\operatorname{argmin}} f(x)$, then $f(r)\geq f(b)$ ✗
Therefore, $(R,+,\cdot)$ is a PID

Thm. $\mathbb{Z}[i]$ is a Euclidian Domain
proof: $\mathbb{Z}[i]=\{a+bi : a,b\in\mathbb{Z}\}$
Let $f:\mathbb{Z}[i]\to\mathbb{N}$ given by $f(z)=|z|^2=a^2+b^2$ ✓
let $x,y\in\mathbb{Z}[i]$, $y\neq 0$, $q,r\in\mathbb{Z}[i]$, $q\in\mathbb{Z}$
Thus $\mathrm{Re}\,x=q\cdot\mathrm{Re}\,y+\mathrm{Re}\,r$, $\mathrm{Im}\,x=q\cdot\mathrm{Im}\,y+\mathrm{Im}\,r$

Thm. $\mathbb{Z}$ is a Euclidian Domain
proof: let $f:\mathbb{Z}\setminus\{0\}\to\mathbb{N}$ given by $f(x)=|x|$
thus it holds

Bezout's Th'm

Let R be an Euclidian domain, then $\forall\, m, n \in R$
$\gcd(m,n) = sm+tn$ for some $s,t \in R$

proof: Given $\nu: R \to \mathbb{N}$

Then $m = q_1 n + r_1$, $\nu(r_1) < \nu(n)$
$n = q_2 r_1 + r_2$, $\nu(r_2) < \nu(r_1)$
$r_1 = q_3 r_2 + r_3$, $\nu(r_3) < \nu(r_2)$

By ascending, $\nu(r_1) > \nu(r_2) > \cdots \geq 0$, $\nu(r_i) \in \mathbb{N}$
So $\exists\, k \in \mathbb{N}$ s.t. r_k is the last nonzero remainder

Claim. $r_k = \gcd(m,n)$

Since $r_{k-1} = q_{k+1} r_k$, then $r_k \mid r_{k-1}$
Say that: $r_k \mid r_{k-i}$ for $\forall\, 1 \leq i \leq k-1$
If $r_k \mid r_{k-1}, r_{k-2}, \cdots, r_{k-i}$, $r_{k-i-1} = q_{k-i+1} r_{k-i} + r_{k-i+1}$, so $r_k \mid r_{k-i-1}$
Therefore $r_k \mid m$ & $r_k \mid n$
And if $c \mid m$ & $c \mid n$, then $c \mid m - q_1 n \Rightarrow c \mid r_1$
$c \mid n - q_2 r_1 \Rightarrow c \mid r_2 \Rightarrow c \mid r_3 \Rightarrow \cdots \Rightarrow c \mid r_k$
Hence $r_k = \gcd(m,n)$
This implies that $\exists\, s,t \in R$, $\gcd(m,n) = sm+tn$

中国剩余定理 (CRT)

Let R be a UFD, $m_1, m_2, \cdots, m_k \in R$ are coprime.
For any fixed $a_1, \cdots, a_k \in R$,

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

has a unique solution under module $M = m_1 \cdots m_k$

proof: Define $M_i = \frac{M}{m_i} = \prod_{j \neq i} m_j$, $\gcd(M_i, m_i) = 1$
Then $\exists\, s_i, t_i \in R$, $s_i M_i + t_i m_i = 1$, so $s_i M_i \equiv 1 \pmod{m_i}$
Let $x = \sum_{i=1}^{k} a_i s_i M_i$ Claim. $x \equiv a_i \pmod{m_i}$
$x - a_i = \sum_{j \neq i} a_j s_j M_j + a_i (s_i M_i - 1)$, Since $m_i \mid \sum_{j \neq i} a_j s_j M_j$, $m_i \mid (s_i M_i - 1)$
Then $m_i \mid (x - a_i)$, i.e. $x \equiv a_i \pmod{m_i}$
Also, if $\forall i$, $x_1 \equiv x_2 \equiv a_i \pmod{m_i}$

Lemma. if $a \mid c$ & $b \mid c$, $\gcd(a,b) = 1$, then $ab \mid c$
Suppose $c = ad$, $b \mid ad$, since $\gcd(a,b) = 1$, then $b \mid d$ (R is a UID)
so $\exists\, e \in R$, $d = eb$, so $c = eab$, i.e. $ab \mid c$

Claim. $M \mid (x_1 - x_2)$.
Since $\gcd(m_i, m_j) = 1$ $(i \neq j)$, then $\prod_{i=1}^{k} m_i \mid (x_1 - x_2)$, i.e. $M \mid (x_1 - x_2)$
so $x_1 \equiv x_2 \pmod{M}$

Def. A ideal M is the maximal ideal of R if $M \neq R$ but M is not contained in any other ideals of R

Cor.

(a) A ideal M of R is maximal iff $\overline{R} = R/M$ is a field

(b) The zero ideal of R is maximal iff R is a field

proof: (a) (=>) $(r+M)\cdot M = M = 0_{R/M}$ $(r+M)\cdot 1 = r+M$

Consider the ideal $(M, r) = \{m+rs \mid m \in M, r \in R\}$, $r \notin M$

Since M is maximal, then $(M, r) = R$, so $1 \in (M, r)$

$\exists s \in R$, s.t. $m+rs = 1$

Then for $r \notin M$, $(r+M)(s+M) = (rs+m)+M = 1+M$

(<=) Since R/M is a field, then $1+M \neq M$, i.e. $1 \notin M$

Therefore $M \neq R$, so M is proper

Also, if $\exists$ ideal I s.t. $M \subsetneq I \subsetneq R$,

Since R/M is a field, then it's ideals are $\{\pi(M), R/M\}$

Define $\pi: R \to R/M$, $r \mapsto r+M$

$\pi(I)$ is an ideal of R/M, this contradicts

(b) (<=) If R is a field, I is a nonzero ideal

Suppose $a \in I \setminus \{0\}$, then $\forall r \in R$, $(r \cdot a^{-1})a = r \in I$, i.e. $R \subseteq I$,

Therefore its maximal ideal is $\{0\}$

(=>) Clearly $0, 1 \in R$

$\forall a \in R \setminus \{0\}$, a is not contained in any proper ideal

Clearly (a) is an ideal of R, $(a) \neq \{0\}$, so $(a) = R$

i.e. $\exists b \in R$, s.t. $ab = 1$

Prop. The maximal ideals of $\mathbb{Z}$ are (p), $p \in \mathbb{P}$

Thm. (CRT) Let R be a ring, $I_1, \cdots, I_n$ be ideals of R, each I_i & I_j are coprime, then

$$R/\bigcap_{k=1}^{n} I_k \cong \bigoplus_{k=1}^{n} R/I_k$$

proof: Construct the homomorphism $\phi: R \to \bigoplus_{k=1}^{n} R/I_k$, $r \mapsto (r+I_1, \cdots, r+I_n)$

Therefore $r \in \ker(\phi)$ iff $r \in \bigcap_{k=1}^{n} I_k$

WTS. ϕ is surjective

It is enough to show that $\exists x \in R$, $\phi(x) = (1, 0, \cdots, 0)$

Take $u_i \in I_1$, $v_i \in I_i$, then let $x = \prod_{i=2}^{n} v_i = \prod_{i=2}^{n} (1-u_i) \equiv 1 \pmod{I_1}$

Therefore $\operatorname{im}(\phi) = \bigoplus_{k=1}^{n} R/I_k$

So $R/\bigcap_{k=1}^{n} I_k \cong \bigoplus_{k=1}^{n} R/I_k$

Chapter 3
Galois Theory

——The zenith of algebra

Goal: FTG (Fundamental Theorem of Galois)
i.e. If I/K is a field extension, then $\exists$ inclusion reversing bijective from intermediate fields $L/M/K$ to subgroups of Galois group $Gal(L/K)$

Assume K is a field $\Leftrightarrow$ $\begin{cases} (K,+) \text{ Abelian group} \\ (K\setminus\{0\},\cdot) \text{ Abelian group} \\ a(b+c)=ab+ac \end{cases}$

$K[x]=\{a_0+\cdots+a_nx^n : a_n\neq 0, a_0,\cdots a_n\in K\}$

Thm. $K[x]$ is a Euclidean Domain

proof: Let $a(x), b(x)\in K[x]$, $b(x)\neq 0$

Let $f: K[x]\setminus\{0\}\longrightarrow \mathbb{N}$ given by $f(p)=\max\{n: p_n\neq 0\}$

Therefore, ① $\deg(a)<\deg(b)$, then $a(x)=0+a(x)$ ✓

② $\deg(a)=\deg(b)$, then $a(x)=\frac{a_n}{b_n}b(x)+(a(x)-\frac{a_n}{b_n}b(x))$

where $\deg(a(x)-\frac{a_n}{b_n}b(x))=\deg(b)-1<\deg(b)$ ✓

③ $\deg(a)>\deg(b)$, let $\deg(a)=m$, $\deg(b)=n$

$a_0+\cdots+a_mx^m=(a_nx^n+\cdots+a_mx^{m+n})+(a_0+\cdots+a_{n-1}x^{n-1})$

$\exists\ q\in K[x]$, where $\deg(q)=m$, s.t. $q(x)\cdot b(x)=a_nx^n+\cdots+a_mx^{m+n}$

Def. $p(x)\in K[x]$ is monic $\Leftrightarrow p(x)=a_0+\cdots+a_nx^n$ & $a_n=1$

Recall. $p(x)\in U \Leftrightarrow p(x)\equiv c$, $c\in K$

Lemma: if $p|(a+b)$ & $p|a, b\neq 0$ then $p|b$

proof: $c_1 p = a+b$, $c_2 p = a$

therefore $(c_1-c_2)p = b$, $p|b$

Cor. if $\deg(P)\geq 1$, then $\exists!\ q(x)$ monic, s.t. $P(x)\sim q(x)$

proof: Let $P(x)=a_0+\cdots+a_n x^n$, $q(x)=\frac{a_0}{a_n}+\cdots+\frac{a_{n-1}}{a_n}x^{n-1}+x^n$

Clearly $P(x)\sim q(x)$

if $P(x)\sim q(x)\sim r(x)$, q, r both monic

then $\begin{cases} q(x)=b_0+\cdots+b_{n-1}x^{n-1}+x^n \\ r(x)=d_0+\cdots+d_{n-1}x^{n-1}+x^n \end{cases}$

Since $q(x)\sim r(x)$, $\exists c\in U$ s.t. $q(x)=cr(x)$

$b_0+\cdots+b_{n-1}x^{n-1}+x^n = c(d_0+\cdots+d_{n-1}x^{n-1}+x^n)$

Hence $c=1$, so $(b_0-d_0)+(b_1-d_1)x+\cdots+(b_{n-1}-d_{n-1})x^{n-1}=0$

Thus $\forall i$, $b_i=d_i$, so $q(x)=r(x)$

Therefore, $\exists!\ q(x)$ monic, s.t. $P(x)\sim q(x)$

Gauss Lemma

If $a(x)\in\mathbb{Z}[x]$ irreducible, then $a(x)\in\mathbb{Q}[x]$ irreducible

proof by contradiction

if $a(x)=a_0+\cdots+a_n x^n$ is irreducible in $\mathbb{Z}[x]$, but reducible in $\mathbb{Q}[x]$

Say $a(x)=b(x)\cdot c(x)$, where $b(x), c(x)\notin U$, $b(x), c(x)\in\mathbb{Q}[x]$

Let $b(x)=b_0+\cdots+b_m x^m\in\mathbb{Q}[x]$, $c(x)=c_0+\cdots+c_k x^k\in\mathbb{Q}[x]$, $b_m, c_k\neq 0$

let n be the product of dominators in bc, then $na(x)=d(x)e(x)$

$d(x)=d_0+\cdots+d_m x^m$, $e(x)=e_0+\cdots+e_k x^k$ $d(x), e(x)\in\mathbb{Z}[x]$

Claim: if $p|n$, then $p|d_0,\cdots,d_m$ or $p|e_0,\cdots,e_k$ $(p\in\mathbb{P})$

proof by contradiction. Assume $p|n$

& Let i,j be the smallest $p\nmid d_i$ & $p\nmid e_j$

Since $a(x)\in\mathbb{Z}[x]$, then $a_{i+j}\in\mathbb{Z}$, $p|n \Rightarrow p|n\cdot a_{i+j}$ ✓

$d(x)e(x)=\sum_{l=0}^{m+k}\left(\sum_{k_1+k_2=l} d_{k_1}e_{k_2}\right)x^l$, then $n\,a_{i+j}=\sum_{k_1+k_2=i+j} d_{k_1}e_{k_2}$

so $p\,|\sum_{k_1+k_2=i+j} d_{k_1}e_{k_2}$, since $p\,|\sum_{k_1+k_2=i+j,\,k_1\neq i} d_{k_1}e_{k_2}$, then $p|d_i e_j$

So $p \mid d_i$ or $p \mid e_j$, this is a contradiction

Therefore the claim is proved now.

let $n = p_1^{s_1} \cdots p_t^{s_t}$, $p_1^{s_1} \cdots p_t^{s_t} a(x) = d(x)e(x)$

Since $p_1, \cdots, p_t \in \mathcal{P}$, while $p_1 \cdots p_t \mid n$, then $a(x) = d^*(x)e^*(x)$

where $d^*, e^* \in \mathbb{Z}[x]$, which contradicts X

so the lemma is proved.

Eisenstein's Irreducibility Criterion

If $a(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x]$. $(a_n \neq 0)$ & $\exists\, p \in \mathcal{P}$ s.t.

(1) $p \nmid a_n$ (2) $p \mid a_0, \cdots, a_{n-1}$ (3) $p^2 \nmid a_0$

Then $a(x)$ is irreducible over $\mathbb{Q}$

proof: Assume $a(x) = b(x)c(x)$ & $\deg(b), \deg(c) \geq 1$, $a_0 \neq 0$

where $\begin{cases} b(x) = b_0 + b_1 x + \cdots + b_m x^m \in \mathbb{Q}[x] \\ c(x) = c_0 + c_1 x + \cdots + c_k x^k \in \mathbb{Q}[x] \end{cases}$, $b_m, c_k \neq 0$, $m+k = n$

so $p \mid b_0 c_0$, $p \mid (b_0 c_1 + b_1 c_0), \cdots, p \mid (b_m c_{k-1} + b_{m-1} c_k)$, $p \nmid b_m c_k$

Since $p^2 \nmid a_0$, then $(p \mid b_0 \overset{*\text{WLOG}}{\&}\ p \nmid c_0)^*$ or $(p \mid c_0 \,\&\, p \nmid b_0)$

Thus we have $p \mid b_0$, let b_i be the first one s.t. $p \nmid b_i$ $(i < m)$

then $p \mid b_i c_0 + \cdots + b_0 c_i \Rightarrow p \mid b_i c_0 \Rightarrow p \mid c_0$, this is impossible X

if $k \geq 1$ then $p \mid b_0 \Rightarrow p \mid b_1 \Rightarrow \cdots \Rightarrow p \mid b_m$ X

so $k = 0$, i.e. $m = n$, thus $a(x) = c_0 b(x)$, $c_0 \in \mathbb{Q}$

Since $a(x) \neq 0$, then $c_0 \neq 0$, thus c_0 is unit

hence we have $a(x)$ irreducible in $\mathbb{Q}$

Ex. if $K<M<L$, then

$L:K = L:M \circ M:K$

proof: $L:K: K \to L$

$M:K: K \to M$, $L:M: M \to L$

$\forall x \in K$, $M:K(x) = x \in M$

$\forall x \in M$, $L:M(x) = x \in L$

thus $L:K(x) = L:M \circ M:K(x) = x \in L$

Ex. Let $L_1 = \{a+b\sqrt[3]{2}+\sqrt[3]{4} : a,b \in \mathbb{Q}\}$

then $L_1 = \mathbb{Q}[\sqrt[3]{2}]$

Ex. $[\mathbb{C}:\mathbb{R}]=2$

$\mathbb{C} = \{a+bi : a,b \in \mathbb{R}\} = \text{span}(1, i)$

Ex. $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$

$\mathbb{Q}(\sqrt[3]{2}) = \text{span}(1, \sqrt[3]{2}, \sqrt[3]{4})$

Thm. $\mathbb{Q}$ is the smallest field in $\mathbb{C}$

proof: if $K \subset \mathbb{C}$ is a field, then $0, 1 \in K$

Since $(K,+)$ is an abelian group, then $\mathbb{Z} \subset K$

$\Rightarrow p, q \in \mathbb{Z}$, $q \neq 0$, $\Rightarrow \frac{p}{q} \in K$, thus $\mathbb{Q} \subset K$

so $\mathbb{Q}$ is the smallest field in $\mathbb{C}$

Def. if $K<L<\mathbb{C}$, then

$L:K$ is called a field extension $\Leftrightarrow$

$L:K = i:K \xrightarrow{\text{Hom}} L$, i.e. $\forall x \in K$, $i(x) = x \in L$

Def. $L:K$ is a simple extension $\Leftrightarrow$

$\exists \alpha \in L$, s.t. $L = K[\alpha]$ (Also written as $K(\alpha)$)

Def. If $L:K$ is a field extension, then

L is a vector space over K

Let $[L:K]$ = dimension of L over K

Thm. (Tower Law) if $K<M<L$

then $[L:K] = [L:M] \cdot [M:K]$

proof: Take $\{u_1, \cdots, u_m\} \subset L$, basis of L over M

Take $\{v_1, \cdots, v_n\} \subset M$, basis of M over K

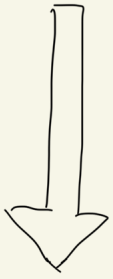
Claim. $\{u_i v_j : 1 \le i \le m, 1 \le j \le n\}$ is a basis of L over K

① if $w \in L$, Check $w \in \text{span}\{u_i v_j : 1 \le i \le m, 1 \le j \le n\}$

$w = a_1 u_1 + \cdots + a_m u_m$, let $a_i = \sum_{j=1}^{n} b_{ij} v_j$

thus $w = \sum_{i=1}^{m} (\sum_{j=1}^{n} b_{ij} v_j) u_i = \sum_{i=1}^{m} \sum_{j=1}^{n} b_{ij} (u_i v_j)$, Therefore $w \in \text{span}(u_i v_j)$

② Check that $\{u_i v_j : 1 \le i \le m, 1 \le j \le n\}$ is linearly independent



Cor. , if $K_0 < \cdots < K_n$
then $[K_n : K_0] = [K_n : K_{n-1}] \cdots [K_1 : K_0]$

$\{p(x)q(x) : q(x) \in K[x]\}$

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

Let $w=0$, i.e. $\sum_{i=1}^{m}(\sum_{j=1}^{n} b_{ij}v_j)u_i = 0$
Since $\{u_1, \cdots, u_m\}$ is a basis, therefore $\sum_{j=1}^{n} b_{ij}v_j = 0$
Since $\{v_1, \cdots, v_n\}$ is a basis, therefore $b_{ij} = 0$
thus $\{u_i v_j : 1 \le i \le m, 1 \le j \le n\}$ is linearly independent
therefore it is a basis
And hence, $[L : K] = [L : M][M : K]$

Def. if $K < \mathbb{C}$ & $\alpha \in \mathbb{C}$, then α is algebraic over K
$\Leftrightarrow \exists\, p(x) \in K[x] \setminus \{0\}$, s.t. $P(\alpha) = 0$

Def. if α is algebratic over $K < \mathbb{C}$
then $m_{K(\alpha)}(x)$ is the minimal polynomial of α over K
$\Leftrightarrow m_{K(\alpha)}(x)$ is the monic polynomial with least degree s.t. $m(\alpha) = 0$
Check. $m(x)$ exists & unique.
proof: Let $I = \{p(x) \in K[x] : p(\alpha) = 0\}$
Let $f : K[x] \xrightarrow{\text{Hom}} K[\alpha]$ be given by $f(p) = p(\alpha)$
Thus we have $I = \ker(f) \lhd K[x]$
Since $K[x]$ is an Euclidian Domain, then it is a PID
Therefore $\exists\, p(x)$, s.t. $I = (p(x))$
Let $m(x) \sim p(x)$ and $m(x)$ is monic, thus we have $m(x)$ unique
(WLOG $\deg(p) = n$, then $\exists\, q(x) \equiv c$, s.t. $\deg(m) = \deg(p)$)

Ex. $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=4$

$m_{\mathbb{Q}}(\sqrt{2}+\sqrt{3})=x^4-10x^2+1$

clearly $\deg(m_{\mathbb{Q}}(\sqrt{2}+\sqrt{3}))=4$

$[\mathbb{Q}[\sqrt[3]{2}]:\mathbb{Q}]=3$

Since $m_{\mathbb{Q}}(\sqrt[3]{2})=x^3-2$

$\deg(m_{\mathbb{Q}}(\sqrt[3]{2}))=3$

Ex. $[\mathbb{Q}[\sqrt{2},i]:\mathbb{Q}]=?$

By tower law

$[\mathbb{Q}[\sqrt{2},i]:\mathbb{Q}]=[\mathbb{Q}[\sqrt{2},i]:\mathbb{Q}[\sqrt{2}]]\cdot[\mathbb{Q}[\sqrt{2}]:\mathbb{Q}]$

Clearly $[\mathbb{Q}[\sqrt{2}]:\mathbb{Q}]=2$

then find $[\mathbb{Q}(\sqrt{2},i):\mathbb{Q}(\sqrt{2})]$

$m_{\mathbb{Q}(\sqrt{2})}(i)=x^2+1$

thus $[\mathbb{Q}(\sqrt{2},i):\mathbb{Q}(\sqrt{2})]=2$

so $[\mathbb{Q}(\sqrt{2},i):\mathbb{Q}]=4$

Thm. if $\alpha\in\mathbb{C}$, $K(\alpha):K$ is a simple extension

then $[K(\alpha):K]=\deg m_K(\alpha)(x)$

proof: Case 1 if α is transcendental over K

then $[K(\alpha):K]=\deg m_K(\alpha)=\infty$

Case 2 if α is algebraic

let $m_K(\alpha)=a_0+\cdots+a_{n-1}x^{n-1}+x^n$

Claim. $\{1,\alpha,\cdots,\alpha^{n-1}\}$ is a basis of $K(\alpha)$ over K

Check. $\{1,\alpha,\cdots,\alpha^{n-1}\}$ is linearly independent

Since $m_K(\alpha)$ is the polynomial with the least degree of α

then $a_0+\cdots+a_{n-1}\alpha^{n-1}=0 \Leftrightarrow a_0=a_1=\cdots=a_{n-1}=0$

Therefore $\{1,\alpha,\cdots,\alpha^{n-1}\}$ is linearly independent

Check. $\operatorname{span}\{1,\alpha,\cdots,\alpha^{n-1}\}=K[\alpha]$

Assume $z=b_0+b_1\alpha+\cdots+b_m\alpha^m$, $m\in\mathbb{N}$, $z\in K(\alpha)$

Since $K[x]$ is a Euclidian domain, then

$p(x)=q(x)m_K(\alpha)(x)+r(x)$, where $r(x)=0$ or $\deg(r)<\deg(m_K(\alpha))=n$

$(p(x)=b_0+b_1x+\cdots+b_mx^m)$, so $\deg(r)\le n-1$

then $z=r(\alpha)\in\operatorname{span}(1,\alpha,\cdots,\alpha^{n-1})$

so $\{1,\alpha,\cdots,\alpha^{n-1}\}$ is a basis for $K[\alpha]$ over K

thus we have $[K[\alpha]:K]=\deg(m_K(\alpha))$

Ex. $Aut(\mathbb{C}/\mathbb{R}) \cong C_2$

proof: if $f: \mathbb{C} \xrightarrow{iso} \mathbb{C}$ $\mathbb{R}$-aut~

$\forall x \in \mathbb{R}$, $f(x)=x$

$f(i)^2 = f(i^2) = f(-1) = -1$

then $f(i) = \pm i$

$f(a+bi) = f(a) + f(b)f(i) = a \pm bi$

if $f(i)=i$, then $f(z)=z$

if $f(i)=-i$, then $f(z)=\bar{z}$

then

$\circ$	id	conj
id	id	conj
conj	conj	id

$\cong C_2$

Ex $Aut(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong C_2$

if $f: \mathbb{Q}(\sqrt{2}) \xrightarrow{iso} \mathbb{Q}(\sqrt{2})$ is a $\mathbb{Q}$-auto

then f bij. f hom.

& $f(a+b\sqrt{2}) = a + bf(\sqrt{2})$

$f(\sqrt{2})^2 = f(2) = 2$, then $f(\sqrt{2}) = \pm\sqrt{2}$

$\circ$	+	−
+	+	−
−	−	+

$\cong C_2$

Eg. for $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$

① $\mathbb{Q}(\sqrt{2})$ is an intemediate field

② $\mathbb{Q}(i)$ is also an ~

Def. if $L:K$ is a field extension, then

$f: L \to L$ is a K-automorphism <=>

<=> ① $f: L \xrightarrow{iso} L$

② $f|_K = id_K$

Def. if $L:K$ is a field extension, then

$Aut(L/K) = \{f: L \to L$ K-automorphism$\}$

Note that L/K field extension <=> $L:K$ field extension

Called the automorphism group of L/K

Check. if $L:K$ is a field extesion

then $(Aut(L/K), \circ)$ is a group.

⓪ if $f, g: L \xrightarrow{iso} L$ K-automorphism,

then $f, g: L \xrightarrow{iso} L \Rightarrow f \circ g: L \xrightarrow{iso} L$ $f \circ g|_K = id_K$

① Clearly $f \circ (g \circ h) = (f \circ g) \circ h$

② Since $f: L \xrightarrow{iso} L$, then $\exists f^{-1}: L \xrightarrow{iso} L$, $f \circ f^{-1} = id_L = f^{-1} \circ f$

③ $id_L \circ f = f \circ id_L$

Def. if L/K is a field extension, then M is an intermediate field of L/K <=> $K < M < L$

Def. if $K < \mathbb{C}$, $f \in K[x]$, the f splits over K <=>

$f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$, where $c, \alpha_1, \cdots, \alpha_n \in K$

Ex. Σ exists & is a field

proof: By FTA, $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ WLOG $c=1$

$= c_0 + \cdots + c_{n-1}x^{n-1} + x^n$, $c_i \in K$, $\alpha_i \in \mathbb{C}$

$K(\alpha_1) \subset K(\alpha_1,\alpha_2) \subset \cdots \subset K(\alpha_1,\cdots,\alpha_n) \subset \mathbb{C}$

Hence every chain has an upper bound

Therefore by Zorn's Lemma

$\exists \Sigma$ to be the maximal element of the chain

Since every element in the chain is a field

then Σ is also a field

suppose Σ is not the splitting field

then $\Leftrightarrow \alpha_i$ s.t. $\Sigma \subset \Sigma(\alpha_i)$, which contradicts

Ex. Find splitting field of x^3-1 over $\mathbb{Q}$

$x^3-1 = (x-1)(x-e^{\frac{2\pi}{3}i})(x-e^{\frac{4\pi}{3}i})$

So the splitting field is

$\mathbb{Q}(1, e^{\frac{2\pi}{3}i}, e^{\frac{4\pi}{3}i}) = \mathbb{Q}(e^{\frac{2\pi}{3}i})$

$= \mathbb{Q}(-\frac{1}{2} + \frac{\sqrt{3}}{2}i)$

Find the splitting field of x^4+x^2 over $\mathbb{Q}$

$x^4+x^2 = x^2(x+i)(x-i)$

thus the splitting field is $\mathbb{Q}(i)$

Ex. $\mathbb{Q}(\sqrt[3]{2})$ is not normal

proof: Take $f(x) = x^3-2$

Then the roots are

$\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}, \sqrt[3]{2}\zeta^2$. where $\zeta \in \mathbb{C}$ & $\zeta \notin \mathbb{Q}(\sqrt[3]{2})$

hence $\mathbb{Q}(\sqrt[3]{2})$ is not normal

Thm. f splits over $K \Leftrightarrow$ all zeros of f lies in K

proof: By Fundamental Theorem of Algebra, $f \in \mathbb{C}[x] \Rightarrow$

$f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$, where $x-\alpha_i$ are irreducible, $\alpha_i \in \mathbb{C}$

f splits over $K \Leftrightarrow f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$, $\alpha_i \in K$

Since $K[x]$ is a UFD, then the factorization is unique

thus f splits over $K \Leftrightarrow$ all zeros of f lies in K

Def. if $K < \mathbb{C}$, $f(x) \in K[x]$, then Σ is a splitting field for f

$\Leftrightarrow$ ① $K < \Sigma$.

② Σ is the smallest field where f split in Σ.

Thm. if $K < \mathbb{C}$, $f(x)$ has distinct roots $\alpha_1, \cdots, \alpha_n \in \mathbb{C}$

then $\Sigma = K(\alpha_1, \cdots, \alpha_n)$

proof: Clearly, $f(x)$ splits in $K(\alpha_1, \alpha_2, \cdots, \alpha_n)$

WTS. Σ is the smallest

proof: if f splits in M, then $\alpha_1, \alpha_2, \cdots, \alpha_n \in M$ & $K < M$

Since M is a field, then $K(\alpha_1, \cdots, \alpha_n) \subset M$

Def. if Σ/K is a field extension, then

Σ/K normal $\Leftrightarrow$

(if $f(x) \in K[x]$ is irreducible & at least one zero $\in \Sigma$

then $f(x)$ splits in Σ)

($\forall f(x) \in K[x]$ irreducible, if at least one zero of $f(x)$ is in Σ,

then $f(x)$ splits in Σ)

Thm. $\forall K < \mathbb{C}$, $\mathbb{C}/K$ is normal

proof: By FTA, this is trivial

Def. if $L:K$ is a field extension, then $f:L\to L$ is a K-automorphism $\Leftrightarrow$
$\Leftrightarrow$ ① $f:L \xrightarrow{\text{iso}} L$
② $f|_K = id_K$

Def. if $L:K$ is a field extension, then
$Aut(L/K) = \{f:L\to L \text{ } K\text{-automorphism}\}$

Def. The characteristic of F is the smallest integer s.t.
$\underbrace{1+1+\cdots+1}_{p} = 0$

Def. if $K<\mathbb{C}$, $f(x)\in K[x]$ irreducible, then
$f(x)$ is seperable over $K \Leftrightarrow f(x)$ has simple zeros in $\mathbb{C}$
i.e. $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$, where $\alpha_1,\cdots,\alpha_n \in \mathbb{C}$ are distinct

Def. if L/K is a field extension, then L/K separable
$\Leftrightarrow \forall \alpha\in L$, $m_K(\alpha)$ is separable

Def. if L/K is a field extension,
then L/K is a Galois extension $\Leftrightarrow$
① L/K is normal
② L/K is seperable

Def. if L/K is a Galois extension, $L<\mathbb{C}$, then
$Gal(L/K) := Aut(L/K) = \{f:L\to L \text{ } K\text{-automorphism}\}$

Def. if L/K is a field extension, then
L/K is simple $\Leftrightarrow L = K(\alpha)$, $\alpha\in L$
L/K is finite $\Leftrightarrow L = K(\alpha_1,\cdots,\alpha_n)$, $\alpha_1,\cdots,\alpha_n \in L$

Ex. Simplify extensions

$\mathbb{Q}(\sqrt{2}, \sqrt{3})$

x^2-2 x^2-3

take $t \neq \pm \frac{\sqrt{3}}{3}$

Take $c = \sqrt{2}+\sqrt{3}$

Then $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$

Check

basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

: $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$

basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

$(1, \sqrt{2}+\sqrt{3}, 5+\sqrt{6}, 11\sqrt{2}+9\sqrt{3})$

$\mathbb{Q}(\sqrt{3}, i)$

x^2-3 x^2+1

take $t \neq 0$ & $\sqrt{3}i$

let $t = 114514$

so $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\sqrt{3}+114514i)$

Thm. if $K < L < \mathbb{C}$, then L/K simple $\Leftrightarrow$ L/K finite

proof: "$\Rightarrow$" ✓

"$\Leftarrow$" Check for case $n=2$, then use induction

WTS: if $L = K(a, b)$, then $\exists\, c \in L$ s.t. $K(a, b) = K(c)$

Let $A(x) = m_{K(a)}(x)$, $B(x) = m_{K(b)}(x)$

minimal polynomial of a, b over K

If roots of $\begin{cases} A(x) \text{ are } \alpha_1, \cdots, \alpha_m \text{ distinct} \\ B(x) \text{ are } \beta_1, \cdots, \beta_n \text{ distinct} \end{cases}$

Take $t \in K$ s.t. $t \neq \frac{a-\alpha_i}{\beta_j - b}$, $\forall i, j \neq 1$, WLOG $\alpha_1 = a$, $\beta_1 = b$

Let $c = a + tb$

Claim: $K(c) = K(a, b)$

Clearly $c \in K(a, b)$, so $K(c) \subset K(a, b)$

Let $h(x) = A(c - tx)$, Then $h(b) = A(c - tb) = A(a) = 0$

But $\forall j \neq 1$, $h(b_j) = A(c - tb_j) \neq A(a) = 0$

$\Rightarrow$ b is the only common root of $h(x)$ & $B(x)$

Check 1. $b \in K(c)$

Let $p(x) = m_{K(c)}(b)(x)$, then $p(x) \mid B(x)$ & $p(x) \mid h(x)$

So $p(x) \mid \gcd(B(x), h(x)) = (x-b)$

Since p is monic, then $p(x) = x - b$

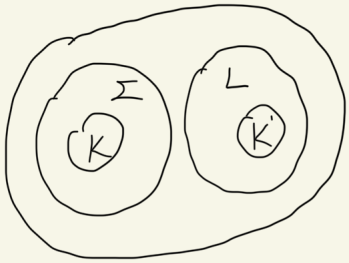
Therefore $[K(b, c) : K(b)] = 1$, thus $b \in K(c)$

Check 2 $a \in K(c)$

Similar method as we show that $b \in K(c)$

Since, $a, b \in K(c)$, therefore $K(a, b) \subset K(c)$

so $\exists\, c \in K(a, b)$, s.t. $K(a, b) = K(c)$



Thm. if L/K is a field extension, $L < \mathbb{C}$, then L/K finite & normal $\Leftrightarrow$ L/K is a splitting field for some $f(x) \in K[x]$

Lemma. If $i: K \xrightarrow{iso} K'$, where $K, K' < \mathbb{C}$ & $f(x) \in K[x]$ & $\Sigma \supset K$ be the splitting field for f. If L is an extension field of K' s.t. $i(f)$ splits over L, then $\exists j: \Sigma \xrightarrow[inj]{hom} L$ s.t. $j|_K = i$

proof: Induction on $[\Sigma : K]$

when $[\Sigma : K] = 1$, $\Sigma = K$, then $i(f)$ splits on over K' so let $j = i$, then it holds

Suppose the lemma holds when $[\Sigma : K] \leq n$, then when $[\Sigma : K] = n+1$

Since $[\Sigma : K] > 1$, f doesn't split over K, thus $\exists \alpha \in \Sigma$, s.t. $f(\alpha) = 0$

let $p(x) \in K$ be the smallest polynomial of α, i.e. $m_K(\alpha)$, so $p(x) | f(x)$

Clearly $p(x)$ is irreducible on K, so $\deg(p) \geq 2$

$i: K \xrightarrow{iso} K'$, so $p(x) | f(x) \Rightarrow i(p)(x) | i(f)(x)$, $i(p)(x) \in K'[x]$

Since $p(x)$ is irreducible, then $K(\alpha) \simeq K/(p(x))$

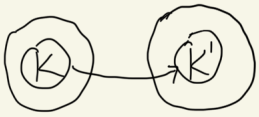
Let $\beta \in L$ be a root for $i(p)(x)$

then $\exists\, \sigma: K(\alpha) \to L$, s.t. $\sigma|_K = i$, $\sigma(\alpha) = \beta$

Denote $M = \sigma(K(\alpha)) = K'(\beta) \subset L$

$[\Sigma : K(\alpha)] = \frac{[\Sigma : K]}{[K(\alpha) : K]} \leq \frac{n+1}{2} < n+1$. Since L is a splitting field for $i(p)$, then $\exists j': \Sigma \to L$, s.t. $j'|_{K(\alpha)} = \sigma$

let $j = j'$, therefore $j|_K = i$



Lemma. If $i: K \xrightarrow{iso} K'$, $K, K' < \mathbb{C}$, $f(x) \in K[x]$, Σ is the splitting field of f over K. Then $\exists\, \Sigma' \supset K'$, s.t. $i(f)$ splits in Σ' & $\exists j: \Sigma \xrightarrow{iso} \Sigma'$ s.t. $j|_K = i$

proof: Induction on $n = \deg f$

if $n=1$, then $\Sigma = K$, $\Sigma' = K'$, ✓

Suppose the lemma holds when $\deg f \leq n-1$, then when $\deg f = n$

Since f doesn't split over K, $\alpha \in \Sigma$ & $\alpha \notin K$ s.t. $f(\alpha) = 0$

Let $p(x) \in K[x]$ be the smallest polynomial of α, i.e. $p = m_K(\alpha)$

$f(x) = a_0 + \cdots + a_n x^n$, then $i(f)(x) = i(a_0) + \cdots + i(a_n) x^n$

Since $i: K \xrightarrow{iso} K'$, then $i(p) \in K'$ is also an irreducible polynomial

Since $i(f)$ splits over Σ', $i(p) \mid i(f)$, then $\exists\, \beta \in L$, $i(p)(\beta) = 0$

Consider $E = K(\alpha)$ & $E' = K'(\beta)$, $E \simeq K[x]/(p(x))$, $E' \simeq K'[x]/(i(p)(x))$

Define $\phi: E \xrightarrow{iso} E'$ by $\phi|_K = i$, $\phi(\alpha) = \beta$

$f(x) = (x-\alpha)g(x)$ in $E[x]$, while $\deg g = \deg f - 1 = n-1$

$\phi(f)(x) = (x-\beta)\phi(g)(x)$, where $\phi(g)(x)$ splits over Σ

Thus $\exists\, j': \Sigma \xrightarrow{iso} \Sigma'$, s.t. $j'|_E = \phi$

Let $j = j'$, then $\exists j: \Sigma \xrightarrow{iso} \Sigma'$, s.t. $j|_K = i$

Lemma. If L/K is a field extension, $L < \mathbb{C}$, & L is a splitting field for $f(x) \in K[x]$. $g(x) \in K[x]$ is irreducible & θ_1, θ_2 are roots of g, then $[L(\theta_1) : L] = [L(\theta_2) : L]$

proof: Since $[K(\theta_1) : K] = [K(\theta_2) : K] = \deg g$, then $K(\theta_1) \simeq K(\theta_2)$

Since $L(\theta_1)$ is a splitting field for g in $K(\theta_1)$

$L(\theta_2)$ is a splitting field for g in $K(\theta_2)$

then by the previous lemma, $L(\theta_1) \simeq L(\theta_2)$

therefore $[L(\theta_1) : L] = [L(\theta_2) : L]$

Ex. Find $Gal(\mathbb{Q}(\sqrt{3}, i):\mathbb{Q})$

Since $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\zeta)$, $\zeta = e^{\frac{2\pi i}{3}}$

$\mathbb{Q}(\zeta) = \{a + b\zeta + c\zeta^2 : a, b, c \in \mathbb{Q}\}$

So if $f: \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ is $\mathbb{Q}$-automorphism

then $f(a) = a$, $\forall\, a \in \mathbb{Q}$

Consider that $(f(\zeta))^3 = f(\zeta^3) = f(1) = 1$

So $f(\zeta) = 1$ or ζ or ζ^2

Case1 $f(\zeta) = 1$, X

Case2 $f(\zeta) = \zeta^2$, then $f(\zeta^2) = \zeta^4 = \zeta$

Case3 $f(\zeta) = \zeta$, then $f(\zeta^2) = \zeta^2$, $f = id$

Therefore $Gal(\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}) \cong C_2$

Recall: automorphism $\Leftrightarrow$

Thm. if L/K is a field extension, $L < \mathbb{C}$, then L/K finite & normal $\Leftrightarrow$ L/K is a splitting field for some $f(x) \in K[x]$

proof: "$\Rightarrow$" if L/K is a field extension, & L/K is finite and normal, let $L = K(\alpha_1, \cdots, \alpha_n)$

Let $P_i = m_K(\alpha_i)$, Let $f(x) = P_1(x) \cdots P_n(x)$

then clearly L is a splitting field for $f(x)$ over K

"$\Leftarrow$" if L/K is a splitting field for $f(x) \in K[x]$

Let $\alpha_1, \cdots, \alpha_n$ be roots of $f(x)$, then $L = K(\alpha_1, \cdots, \alpha_n)$

WTS. if $g(x) \in K[x]$ irreducible & g has a root in L, then g splits in L

Assume g is irreducible. Let θ_1, θ_2 be two roots of $g(x)$

where $\theta_1 \in L$ (by assumption)

Then $[L(\theta_1) : L] = 1$, and by previous lemma $[L(\theta_2) : L] = 1$

Hence $\theta_2 \in L$, so all roots in $g(x)$ lies in L

Therefore L/K is normal & finite

Ex $G_K = Gal(L/M)$

$G_L = Gal(L/L) \cong \{e\}$

Def. if L/K is a Galois extension & $L/M/K$ then $G_M := Gal(L/M)$

Recall. L/K is a Galois extension $\Leftrightarrow$ L/K is seperable & normal

Thm. if $L/M/N/K$, i.e $K < N < M < L$

then $\{e\} = G_L < G_M < G_N < G_K$

K-automorphism

Def. If L/K be a Galois extension & $H < Gal(L/K)$
Let $L^H := \{a \in L : \forall f \in H, f(a) = a\}$, is called a fixed field of H

Thm. If $H < Gal(L/K)$, then $K < L^H < L$

proof: Check. $K \subset L^H$

Since $H < Gal(L/K)$, then $\forall f \in H$, $f \in Gal(L/K)$

thus $f|_K = id_K$

So $\forall x \in K \Rightarrow x \in L^H$, thus $K \subset L^H$

Check. L^H is a field

$f(a+b) = f(a) + f(b) = a + b$

$f(ab) = f(a)f(b) = ab$, so if $a, b \in L^H$, $a+b, a \cdot b \in L^H$

$f(1) = 1$, $f(0) = 0$ ✓

$f(a) + f(-a) = f(0) = 0$ ✓ $f(a) \cdot f(a^{-1}) = 1$ ✓

Therefore L^H is a field

Thm. If $H < G < Gal(L/K)$, then $L^G < L^H$

proof: Check. $L^G \subset L^H$

if $a \in L^G$, then $\forall f \in G$, $f(a) = a$

Since $H \in G$, then $\forall f \in H$, $f(a) = a$, thus $a \in L^H$

therefore $L^G \subset L^H$

Ex. Check:

$|Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})| = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]$

proof: Clearly RHS $= \deg m_{\mathbb{Q}}^{(\sqrt{2}+\sqrt{3})} = 4$

$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$

If $f: \mathbb{Q}(\sqrt{2},\sqrt{3}) \xrightarrow{iso} \mathbb{Q}(\sqrt{2},\sqrt{3})$

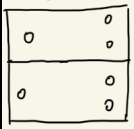
& $f_{\mathbb{Q}} = id_{\mathbb{Q}}$

then $f(a) = a$ for $\forall a \in \mathbb{Q}$

$f(\sqrt{2})^2 = f(2) = 2 \Rightarrow f(\sqrt{2}) = \pm\sqrt{2}$

$f(\sqrt{3})^2 = f(3) = 3 \Rightarrow f(\sqrt{3}) = \pm\sqrt{3}$

thus $|Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})| = 4$



Thm. If L/K is a Galois extension, then

$|Gal(L/K)| = [L:K]$

Assume $[L:K] = n$

L/K Galois $\Rightarrow$ normal $\Rightarrow L$ is a splitting field for $f(x) \in K[x]$

By previous theorem, $\exists \alpha \in L$ s.t. $L = K(\alpha)$

Let $p(x) = m_K(\alpha)(x)$, which is irreducible in K

Then $\deg p = n$, Let β be a root of $p(x)$

Then $K(\alpha) = K(\beta)$ (Since they are both splitting field for $p(x)$)

$\exists j: L \xrightarrow{iso} L$ s.t. $j|_K = id_K$, $j(\alpha) = \beta$

So j is a K-automorphism

Since there are n roots, then $|Gal(L/K)| \geq n$

On the other hand, if $j^*: L \xrightarrow{iso} L$ & $j^*|_K = id_K$

Since $L = K(\alpha)$, & Let $p(x) = c_0 + \cdots + c_n x^n$

$p(\alpha) = 0$, then $c_0 + \cdots + c_n (j^*(\alpha))^n = 0$

ie $j^*(\alpha)$ is a root of $p(x)$, then we have at most n choices

therefore $|Gal(L/K)| = n$

Thm. If L/K is a Galois extension, $K < M < L$, then L/M is a Galois extension.

Check: L/M is seperable

$\forall a \in L$, Let $f(x) = m_K(\alpha)(x)$, which is seperable

Let $g(x) = m_M(\alpha)(x)$. since $K \subset M$, then $g(x) | f(x)$

Since f has simple zeros, then g has simple zeros.

Check L/M is normal

let $h(x) \in M[x]$ irreducible, $\exists \beta \in L$ s.t. $h(\beta) = 0$

Let $p(x) = m_K(\beta)(x) \in K[x]$

Thm. If L is the splitting field of a separable irreducible polynomial $p(x) \in K[x]$, $\deg p = n$, then $Gal(L/K) \cong S_n$

pf: Let $p(x) = (x-c_1)\cdots(x-c_n)$ irreducible, then $\forall i, j$, $K(c_i) = K(c_j)$

so $\forall i, j$, $\exists \varphi \in Gal(L/K)$, $\varphi(c_i) = c_j$

then $\forall i$, $\exists k$, s.t. $c_i = \varphi(c_k)$

Let $C = \{c_1, \cdots, c_n\}$. Then $Gal(L/K) = \{\varphi \mid \varphi: C \xrightarrow{bij} C\}$

so $Gal(L/K) \cong S_n$

Recall: $Gal(L/K)$ is a group

Since L/K is normal, $\beta \in L$, then $p(x)$ splits in L

And since $K \subset M$, then $p(x) \in M[x]$ while $p(\beta)=0$

thus $h(x) \mid p(x)$, therefore $b(x)$ splits in L

Hence L/M is a normal extension

Lemma. If $H < Gal(L/K)$, then $|H| = [L : L^H]$

Assume $H = \{h_1, \cdots, h_r\}$, so $|H| = r$

Since $K < L^H < L$, then L/L^H is a Galois extension

then let $L = L^H(a)$, $p(x) = m_{L^H}(a)(x)$

So $\deg p = [L : L^H]$. Let $b(x) = (x-h_1(a)) \cdots (x-h_r(a))$, where $\deg b = r$

Clearly $id \in Gal(L/L) < Gal(L/L^H)$, then WLOG $h_1 = id$

so $(x-a) \mid b(x) \Rightarrow b(a) = 0$

Since $h_i : L \xrightarrow{iso} L$, then $\exists \bar{h}_i : L[x] \xrightarrow{iso} L[x]$ given by

$\bar{h}_i(a_0 + \cdots + a_n x^n) = h_i(a_0) + \cdots + h_i(a_n) x^n$

Since $b(x) = (x-h_1(a)) \cdots (x-h_r(a))$, then $\bar{h}_i(b(x)) = (x-h_i \circ h_1(a)) \cdots (x-h_i \circ h_r(a))$

Since $H = \{h_1, \cdots, h_r\}$ is a group, then $\{h_i \circ h_1, \cdots, h_i \circ h_r\} = \{h_1, \cdots, h_r\}$

Hence $\bar{h}_i(b(x)) = b(x) \Rightarrow h_i(b_j) = b_j$, so $b(x) \in L^H[x]$

therefore $(x-a) \mid b(x) \Rightarrow p(x) \mid b(x) \Rightarrow \deg p \le r \Rightarrow [L : L^H] \le r$

For each h_i, $\exists j : L \xrightarrow{iso} L$ s.t. $j|_{L^H} = id_{L^H}$, $j(a) = h_i(a)$

Thus $|Gal(L/L^H)| \ge r$, while $|Gal(L/L^H)| = [L : L^H]$ by previous lemma

Therefore, $[L : L^H] = |H| = r$

Lemma. If $H < Gal(L/K)$, then $H = Gal(L/L^H)$

We've shown that $|H| = |Gal(L/L^H)|$

Also, it is clearly that $H \subset Gal(L/L^H)$

thus $H = Gal(L/L^H)$

Cor. If $H < Gal(L/K)$, then $[L^H : K] = \frac{[L:K]}{|H|}$

Thm. $H \mapsto L^H$ & $M \mapsto G_M$ are the inverses of each other (Fundamental Theorem of Galois Theory)

Check. If $L/M/K$, then $L^{G_M} = M$

If $L/M/K$, then $L^{G_M} = \{a \in L : \forall f: L \xrightarrow{iso} L \ \& \ f|_M = id_M, f(a) = a\}$

If $a \in M$, then clearly $a \in L^{G_M}$

If $a \in L^{G_M}$, suppose $a \notin M$, then $\forall f \in Gal(L/M)$, $f(a) = a$

Since $a \notin M$ & $f|_M = id_M$, then $f|_{M(a)} = id_{M(a)}$ for $\forall f \in Gal(L/M)$

Thus $Gal(L/M) \subset Gal(L/M(a))$, which is impossible

therefore $a \in M$, $L^{G_M} \subset M$

So we have $L^{G_M} = M$

Check. If $H < Gal(L/K)$, then $Gal(L/L^H) = H$ (i.e. $G_{L^H} = H$)

This is true by the previous lemma

Fundamental Theorem of Galois Theory ☆

If L/K is a Galois extension, let $G = Gal(L/K)$,

let $\mathcal{F} = \{M : L/M/K\}$, $\mathcal{G} = \{H : H < G\}$. then:

(1) $|G| = [L : K]$

(2) $G_{(-)}$ & $L^{(-)}$ are mutual inverses and they set up an order reversing bijection between $\mathcal{F}$ & $\mathcal{G}$

(3) $M \in \mathcal{F} \Rightarrow [L : M] = |G_M|$

$H \in \mathcal{G} \Rightarrow [L : L^H] = |H|$

(4) M is a normal extension of $K \Leftrightarrow G_M \triangleleft G$

(5) If M is a normal extension of K,

then $Gal(M/K) \simeq G/G_M$

i.e. $Gal(M/K) \simeq Gal(L/K)/Gal(L/M)$

Recall:

If G is a group, then

$N \lhd G \iff \begin{cases} ① \ N < G \\ ② \ \forall a \in G, \ aN = Na \end{cases}$

Lemma. If L/K is a Galois extension, $L/M/K$ & $f \in Gal(L/K)$ then $G_{f(M)} = f G_M f^{-1}$

$f \in Gal(L/K) \Rightarrow f: L \xrightarrow{iso} L$ & $f|_K = id_K$

"$\supset$" If $g \in G_M = Gal(L/M)$, then $g: L \xrightarrow{iso} L$ & $g|_M = id_M$

First. $fgf^{-1}: L \xrightarrow{iso} L$, $\surd$

Next. If $y \in f(M)$, let $x = f^{-1}(y) \in M$

$fgf^{-1}(y) = f \circ g(x) = f(x) \in f(M)$, thus $fgf^{-1}|_{f(M)} = id_{f(M)}$

Thus we have $f G_M f^{-1} \subset G_{f(M)}$

"$\subset$" We show that $f^{-1} G_{f(M)} f \subset G_M$. If $h \in G_{f(M)}$

then $f^{-1} h f: L \xrightarrow{iso} L$ $\surd$. If $x \in M$, let $y = f(x) \in f(M)$

$f^{-1} h f(x) = f^{-1} \circ h(y) = f^{-1}(y) = x \in M$, Thus $f^{-1} G_{f(M)} f \subset G_M$

Therefore $G_{f(M)} = f G_M f^{-1}$

Lemma. If L/K is a Galois extension & $L/M/K$ & M/K normal. $f: M \xrightarrow[inj]{hom} L$ s.t. $f|_K = id_K$, then $f(M) \subset M$

If $\alpha \in M$, let $p(x) = m_K(\alpha)(x)$, $f(p(\alpha)) = p(f(\alpha)) = 0$

So $f(\alpha)$ is a root of $p(x)$, thus $f(\alpha) \in M$ $\surd$

proof of (4): Clearly we have $Gal(L/M) < Gal(L/K)$

Let $f \in G$, then $f G_M f^{-1} = G_{f(M)}$

Since $f: L \xrightarrow{iso} L$ & $f|_K = id_K$, then $f|_M: M \xrightarrow[inj]{hom} L$ & $f|_K = id_K$

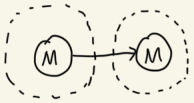
thus we have $f(M) \subset M$, therefore $f G_M f^{-1} \subset G_M$, M normal $\Rightarrow G_M \lhd G$

Conversely, if $Gal(L/M) \lhd Gal(L/K)$

Let $f \in G$, then $f G_M f^{-1} = G_M = G_{f(M)}$, thus $M = f(M)$

Let $g: M \xrightarrow[inj]{hom} L$, s.t. $g|_K = id_K$, then $\exists \bar{g}: L \xrightarrow{iso} L$, $\bar{g}|_K = id_K$

s.t. $\bar{g}|_M = g$, Since $g \in G$, then $M = g(M)$, thus $g: M \xrightarrow{iso} M$, $g|_K = id_K$



Let $b(x) \in K[x]$, irreducible, α, β are roots of $b(x)$, $\alpha \in M$, $\beta \in L$

$\exists\, g: K(\alpha) \xrightarrow{\text{hom}}_{\text{inj}} K(\beta)$ where $g|_K = id_K$, $g(\alpha) = \beta$

Since $\alpha \in M$, $\beta \in L$, then $K(\alpha) \subset M$, $K(\beta) \in L$

so $g: K(\alpha) \xrightarrow[\text{inj}]{\text{hom}} L$, then we have $g(M) = M$

Since $\alpha \in M$, then $\beta = f(\alpha) \in f(M) = M$, so $b(x)$ splits in M

Therefore M/K is normal

proof of (5): Let $f: Gal(L/K) \longrightarrow Gal(M/K)$ given by

$f(\sigma) = \begin{cases} \sigma|_M, & \sigma: M \xrightarrow{\text{iso}} M \\ id|_M, & \text{otherwise} \end{cases}$, then $f: Gal(L/K) \xrightarrow[\text{surj.}]{\text{hom}} Gal(M/K)$

Clear $Im(f) = Gal(M/K)$, $Ker(f) = Gal(L/M)$

(First Group Isomorphism Theorem)

Hence $Gal(L/K)/Gal(L/M) \simeq Gal(M/K)$

Recall: $ax^2+bx+c=0 \ (a \neq 0) \Rightarrow x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$

$x^3+ax+b=0 \Rightarrow$ one solution is $x = \sqrt[3]{-\frac{b}{2}+\sqrt{D}} + \sqrt[3]{-\frac{b}{2}-\sqrt{D}}$, $D = \frac{a^3}{27}+\frac{b^2}{4}$

$ax+b=0 \Rightarrow x = -\frac{b}{a}$

For $x^3+ax+b=0$

$x \in \mathbb{Q}(\sqrt{D}, \sqrt[3]{-\frac{b}{2}+\sqrt{D}}, \sqrt[3]{-\frac{b}{2}-\sqrt{D}})$

Ex.
$\mathbb{Q}\left(\sqrt{D}, \sqrt[3]{-\frac{b}{2}+\sqrt{D}}, \sqrt[3]{-\frac{b}{2}-\sqrt{D}}\right)$
is a radical extension
proof: $(\sqrt{D})^2 = D = \frac{a^3}{27}+\frac{b^2}{4} \in \mathbb{Q}$
$\left(\sqrt[3]{-\frac{b}{2}+\sqrt{D}}\right)^3 = -\frac{b}{2}+\sqrt{D} \in \mathbb{Q}(\sqrt{D})$
$\left(\sqrt[3]{-\frac{b}{2}-\sqrt{D}}\right)^3 = -\frac{b}{2}-\sqrt{D} \in \mathbb{Q}(\sqrt{D}, \sqrt[3]{-\frac{b}{2}-\sqrt{D}})$

Def. $P(x) \in \mathbb{C}[x]$ is solvable by radicals $\Leftrightarrow$
$\exists$ radical expression giving its roots in terms of its coefficients (radical expression: "+" "−" "·" "/" "$\sqrt[n]{\ }$")

Def. $K(C_1, \cdots, C_n)$ is a radical extension $\Leftrightarrow$
$\forall 1 \le i \le n$, $\exists s_i \in \mathbb{N}^+$, s.t. $C_i^{s_i} \in K(C_1, \cdots, C_n)$

Def. $z \in \mathbb{C}$ is an n-th root of unity $\Leftrightarrow z^n = 1$

Thm. (Complex Analysis) z is an n-th root of unity
$\Leftrightarrow z = 1, \omega, \cdots, \omega^{n-1}$, where $\omega = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$

Thm. Clearly $(\{1, \omega, \cdots, \omega^{n-1}\}, \cdot) < \mathbb{C}$

Def. If L/K is a Galois extension, then
L/K is an Abelian extension $\Leftrightarrow$
$Gal(L/K)$ is an Abelian Group

Thm. If ω is primitively n th root of unity, then
$K(\omega)$ is an Abelian extension of K
proof: $K(\omega) = \{a_0 + a_1\omega + \cdots + a_{n-1}\omega^{n-1} : a_0, \cdots, a_{n-1} \in K\}$
Let $f : K(\omega) \xrightarrow{iso} K(\omega)$ given by $f|_K = id_K$, $f(\omega) = \omega^i$ for some i
$g : K(\omega) \xrightarrow{iso} K(\omega)$, $g|_K = id_K$, $g(\omega) = \omega^j$ for some $j \in \mathbb{N}^+$
then $f \circ g(\omega) = g \circ f(\omega) = \omega^{ij}$
Hence $Gal(K(\omega)/K)$ is an Abelian group

Lemma. If $a \in K \setminus \{0\}$, $b^n = a$, then $x^n = a$
$\Leftrightarrow x = b, b\omega, \cdots, b\omega^{n-1}$, where ω is an n^{th} root of unity

Thm. If $c^n=1$ & $\omega \in K$, then $K(c)/K$ is an Abelian extension

proof: Since c is radical, then $m_{K(c)}(x)=x^n-1$

the roots of $m_{K(c)}(x)$ are $c, c\omega, \cdots, c\omega^{n-1} \in K(c)$

Thus $K(c)/K$ is Galois

Let $f \in Gal(K(c)/K)$, then $f: K(c) \xrightarrow{iso} K(c)$, $f|_K = id_K$

$f(c)=c\omega^i$ for some $i \in \{0,1,\cdots,n-1\}$

Then let $g \in Gal(K(c)/K)$, $g(c)=c\omega^j$

so $f\circ g(c)=g\circ f(c)=c\omega^{i+j}$

Therefore $K(c)/K$ is an Abelian extension

Cor. Assume K contains enough primitive roots of unity.

Assume $L=K(c_1,\cdots,c_n)$ is a radical extension

Let $I_i=K(c_1,\cdots,c_i)$, $\forall\ 1\le i\le n$, Then

I_i/I_{i-1} is a normal Abelian extension, $\forall\ 1\le i\le n$

proof: $I_i=I_{i-1}(c_i)$

Since L/K is a radical extension, then $c_i^{s_i} \in I_{i-1}$ for some $s_i \in \mathbb{N}^*$

take $b^{s_i}=a$, then $\frac{c_i}{b}$ is a unit root

Therefore I_i/I_{i-1} is an abelian extension

Cor. $\{e\}=G_{I_n} \lhd \cdots \lhd G_{I_0}=G_K$ & $G_{I_i}/G_{I_{i+1}} \simeq Gal(I_{i+1}/I_i)$

Since I_{i+1}/I_i is normal, then by FTG, $G_{I_{i+1}} \lhd G_{I_i}$

Also by FTG, we have $G_{I_i}/G_{I_{i+1}} \simeq Gal(I_{i+1}/I_i)$

Ex. If L/K is a radical extension, then $Gal(L/K)$ is solvable

Def. G is solvable $\Leftrightarrow \exists$ subgroups $G_0 \cdots G_n < G$, s.t. $\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$, where every G_{I+1}/G_I is Abelian.

Thm. If G is solvable, $f: G \xrightarrow[\text{surj}]{\text{hom}} G'$, then G' is solvable

Lemma. G/H Abelian $\Leftrightarrow \forall x, y \in G,\ xyx^{-1}y^{-1} \in H$

G/H Abelian $\Leftrightarrow \forall x, y \in G.\ (xH)(yH) = (yH)(xH)$

$\Leftrightarrow \forall x, y \in G.\ (xy)H = (yx)H \quad \Leftrightarrow (x^{-1}y^{-1}xy)H = H$

$\Leftrightarrow \forall x, y \in G,\ x^{-1}y^{-1}xy \in H \Leftrightarrow xyx^{-1}y^{-1} \in H$

pf of Thm): Let G be a solvable group

So $\exists G_0, \cdots, G_n < G$, s.t. $G_0 \lhd G_1 \lhd \cdots \lhd G_n \lhd G$ &

G_{i+1}/G_i Abelian, $\forall 1 \le i \le n$. So $\{e\} = f(\{e\}) = G_0'$

Let $f(a) = a'$, $f(e) = e'$, then we have

$\{e'\} < G_0' < \cdots < G_n' < G'$

WTS: $G_i' \lhd G_{i+1}'$, $\forall i$, i.e. $\forall a' \in G_{i+1}'$, $a'G_i' = G_i'a'$ & G_{i+1}/G_i Abelian

Since $G_i \lhd G_{i+1}$, $\forall a \in G_{i+1}$, $aG_i = G_i a$

$f(aG_i) = f(G_i a)$, then $a'f(G_i) = f(G_i)a'$. $a'G_i' = G_i'a'$

Also we know that G_{i+1}/G_i's are Abelian.

WLOG $x, y \in G_{i+1}$, then $xyx^{-1}y^{-1} \in G_i$

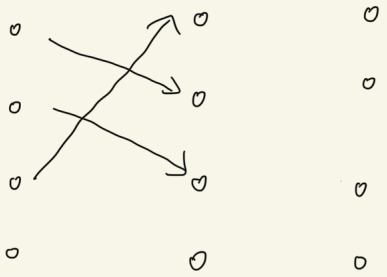
then $f(xyx^{-1}y^{-1}) \in f(G_i) = G_i'$, $x'y'(x')^{-1}(y')^{-1} \in G_{i+1}'$

Hence we have G_{i+1}'/G_i' Abelian.

Therefore G' is solvable

Thm. $P(x) \in K[x]$ & $P(x)$ is solvable by radicals, $\Leftrightarrow$
its Galois group is solvable.
Let M be the splitting field of $P(x)$.
Since $P(x)$ is solvable by radical, then $\exists L = K(c_1, \cdots, c_n)$
is a radical extension of K such that
L is a splitting field for P, then L/K is Galois
By FTG, $G_K / G_M \simeq Gal(M/K)$, $\exists f: G_K \xrightarrow[\text{surj}]{\text{hom}} Gal(L/M)$
Since $Gal(L/K)$ is solvable, then $Gal(L/M)$
is also solvable

$P(x) \in K[x]$ is solvable by radicals $\Leftrightarrow$
its Galois extension is solvable



Eg. S_2 is solvable

Clearly $S_2 = \{e, (1,2)\}$, $|S_2| = 2$

then $\{e\} \lhd S_2$

Also, $S_2/\{e\} = \{\{e\}, \{(12)\}\} \simeq S_2$, which is Abelian

therefore S_2 is solvable

Lemma. $L = K(c_1, \cdots, c_n)$, $Gal(L/K) \simeq S_n$ (L/K radical)

$f: L \xrightarrow{iso} L$, $f|_K = id_K$ is a permutation of $\{c_1, \cdots, c_n\}$

And hence $|Gal(L/K)| = |S_n| = n!$

Thm. S_n is not solvable when $n \geq 5$ ★★★★★ !!!!!

Suppose S_n is solvable, then $\exists N \lhd S$ s.t. S_n/N is abelian

so $\forall x, y \in S_5$, $xyx^{-1}y^{-1} \in N$

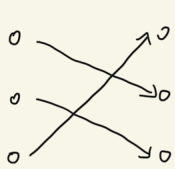
let $x = (abc)$, $y = (aec)$, then $xyx^{-1}y^{-1} = (abc) \in N$

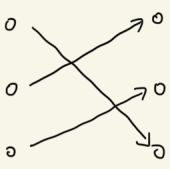
so $\{e\} \neq N$, i.e. $\{e\} \not\lhd S_5$, which contradicts

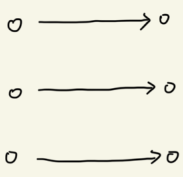
so S is not solvable

This implies that polynomial equations of degree 5 or higher have no radical solutions.

Equations of degree five or higher have no root-finding formula.







$A_3 = \{e, (123), (132)\} \lhd S_3$

$\{e\} \lhd A_3 \lhd S_3$, so S_3 is solvable


"Resistanse"
Seija Kijin