Ring

(1) Elementary:

① Lemma $ab=ac$. If $a, b-c$ are nzd in R. then $b=c$

Cor. i) R is integral domain $\Leftrightarrow$ R satisfies cancellation.
ii) R is finite and no (zero) divisor $\Rightarrow$ R is division ring

② Classification of unitary Ring
- Integral domain: No zero divisors. commutative
- Division ring: nonzero ele is unit
- Field: commutative division ring

(Field = commutative + division ring; UH)

Some special rings:

1. Boolean Ring: $a^2=a$. for all $a \in R$.
then R is commutative and $ata=0$

Pf: $a - a^2 = (-a)^2 = -a \quad \therefore a+a=0$

$(x+y)^2 = (x+y) = x^2+y^2+xy+yx \quad \therefore xy=-yx=yx.$

2. $|R|>1$. If $\forall a\in R.\ a\neq 0.\ \exists$ unique $b\in R$. s.t. $aba=a$.
then R is division ring.

Pf: If a is zero divisor. then $\exists ac=0.\ c\neq 1. \quad \therefore aca=0.$
but $\exists!\ b$. s.t. $aba=a \Rightarrow a(b+c)a=a.\ b+c=b \quad \therefore c=0$
Contradiction! $\therefore R$ has no zero divisor!
Then by $abab=ab \Rightarrow bab=b$. prove: ab is id!
$\forall x\in R,\ babx=bx \quad \therefore abx=x. \quad xaba=xa \quad \therefore xab=x.$

③ Something about homo of Ring. $\varphi: R\to S$

Property: $\varphi(-a)=-\varphi(a).\ \varphi(0)=0$
but $\varphi(1_R)=1_S$ isn't necessary!

1. If φ is epi between unitary ring R, S. then $\varphi(1_R)=1_S$

Pf: Suppose $\varphi(a)=1_S.\ a\neq 1_R$. then $\varphi(1_R)=S\neq 1_S$ ↓ strengthend!
$\therefore \varphi(a\cdot 1_R)=\varphi(a)=S$. Contradiction!

2. If $\forall u$ is unit in R. $f(u)$ is unit in S ⟶ homo- of field: satisfies $f(1_R)=1$!
then $f(1_R)=1_S.\ f(u^{-1})=f^{-1}(u)$

Pf: If $f(1_R)=a$. then a is an unit.
And $f(1_R^2)=a^2=a \quad \therefore a=a^2\cdot a^{-2}=aa^{-2}=1.$
$f(u)=f^{-1}(u^{-1})$ obviously!

3. If $f(r)\neq 0$. for some $r\neq 0$. R has id. S has no zero divisors, then S is a ring with id $f(1_R)$

Pf: Now show $f(1_R) \neq 0$!

④ Characteristics of ring.

Lemma. If R has no zero divisor, then $\operatorname{char} R = n$ / ∞.

Pf: If $|a| = n$. $a \cdot b \neq 0$. $|b| = m$. $\Rightarrow (na)b = a(nb) = 0$

$\therefore nb = 0 \quad \therefore m \mid n$. $(mb)a = mba = b(ma) = 0$.

$\therefore ma = 0 \quad \therefore n \mid m \quad \therefore m = n$.

Cor. n is prime.

Pf: If $n = ab \Rightarrow ab1_R = (a1_R)(b1_R) = 0$

$\therefore a1_R = 0$ or $b1_R = 0$. contradict!

Cor. If $|R| = 2p$.
$\Rightarrow \operatorname{char} R = 2$.
Pf: $(R, +)$ exist an element of order 2!

Theorem. If R is without 1_R. then it can be embedded into S with 1_S. $\operatorname{char} S = 0$ or $\operatorname{char} R$.

pf: $S = R \oplus \mathbb{Z}$ or $R \oplus \mathbb{Z}_{\operatorname{char} R}$. (Abelian group)

Def: multiplication: $(r_1, k_1)(r_2, k_2) = (r_1 r_2 + k_1 r_2 + k_2 r_1, k_1 k_2)$

⑤ nilpotent: a is nilpotent $\Leftrightarrow$ If $a^n = 0 \Rightarrow a = 0$

Pf: ($\in$) If $a^n = 0$. then $\exists N$. st $2^N > n$.

$\therefore a^{2^N} = 0 \Rightarrow a^{2^{N-1}} = 0 \Rightarrow \cdots a^2 = 1 \Rightarrow a = 0$

($\Rightarrow$) trivial!

⑥ Ideal.

Def: left/right ideal I in R.

i) $a, b \in I \Rightarrow a - b \in I$

ii) $a \in I, r \in R \Rightarrow ra / ar \in I$

Remark: If I is proper, then $a \notin I$ when a is unit!

Prime ideal:

0) R is a ring, P is prime ideal if: $P \neq R$.

$AB \subset P \Rightarrow A \subset P$ or $B \subset P$. A, B are ideals (arbitrary)

Cor. If $ab \in P \Rightarrow a \in P$ or $b \in P$, then P is prime ideal

Pf: If $AB \subset P$, $A \not\subset P$, then $\exists a \in A - P$.

$\therefore ab \in P$, for every $b \in B$ $\therefore \forall b \in P \Rightarrow B \subset P$

Cor. If R is commutative, then converse is true.

By $(a)(b) \subset (ab) \subset P$ since $ab \in P$.

$\therefore (a) \subset P$ or $(b) \subset P$.

Remark: other equivalent descriptions:

i) $r, s \in R$, and $rRs \subset P$, then $r \in P$ or $s \in P$

ii) $(r)(s) \subset P \Rightarrow r \in P$ or $s \in P$

iii) U, V are right/left ideals, $UV \subset P \Rightarrow U \subset P$ or $V \subset P$

If: 0) $\Rightarrow$ i) $rRsR \subset rRs \subset P$ $\therefore (rr)RsR \subset P$

$RrR\,RsR \subset rRsR \subset rRs \subset P$ $\therefore RrR\,RsR \subset P$

since RrR or RsR is ideal (check) $\Rightarrow RsR \subset P$.

Or by: $(rq_1)(sq_2) \subset P$, $\forall q_1, q_2 \in R$, If $sR \subset P$

$\Rightarrow RsR \subset P \Rightarrow (s)^3 \subset RsR \subset P$ $\therefore (s) \subset P$, $s \in P$

If $\exists\, sq_2 \notin P \Rightarrow \forall q_1 \in R$. $rq_1 \in P$ $\therefore rR \subset P$ ✓

i) $\Rightarrow$ 0) $AB \subset P \Rightarrow$ By $AR \subset A$. $\therefore ARB \subset AB \subset P$

$\therefore \forall a \in A, b \in B$, $aRb \subset P$, If $\exists b_0 \notin P$, fix $b_0 \Rightarrow \forall a \in P$.

Otherwise $\forall b \in B$. $b \in P$ $\therefore B \subset P$!

i) ⇒ ii) trivial. ii) ⇒ i) $AB \subset P$. then $\forall a \in A, b \in B$.

$(a) \subset A$, $(b) \subset B$, $\therefore (a)(b) \subset P \Rightarrow (a) \subset P$ or $(b) \subset P$.

Exists $b \notin P$. Otherwise $B \subseteq P$. similar argu!

i) ⇒ iii) $U V \subset P$. ⇒ By $UR \subset U$.

$\therefore URV \subset UV \subset P$ $\therefore (RU)(RV) \subset RP \subset P$.

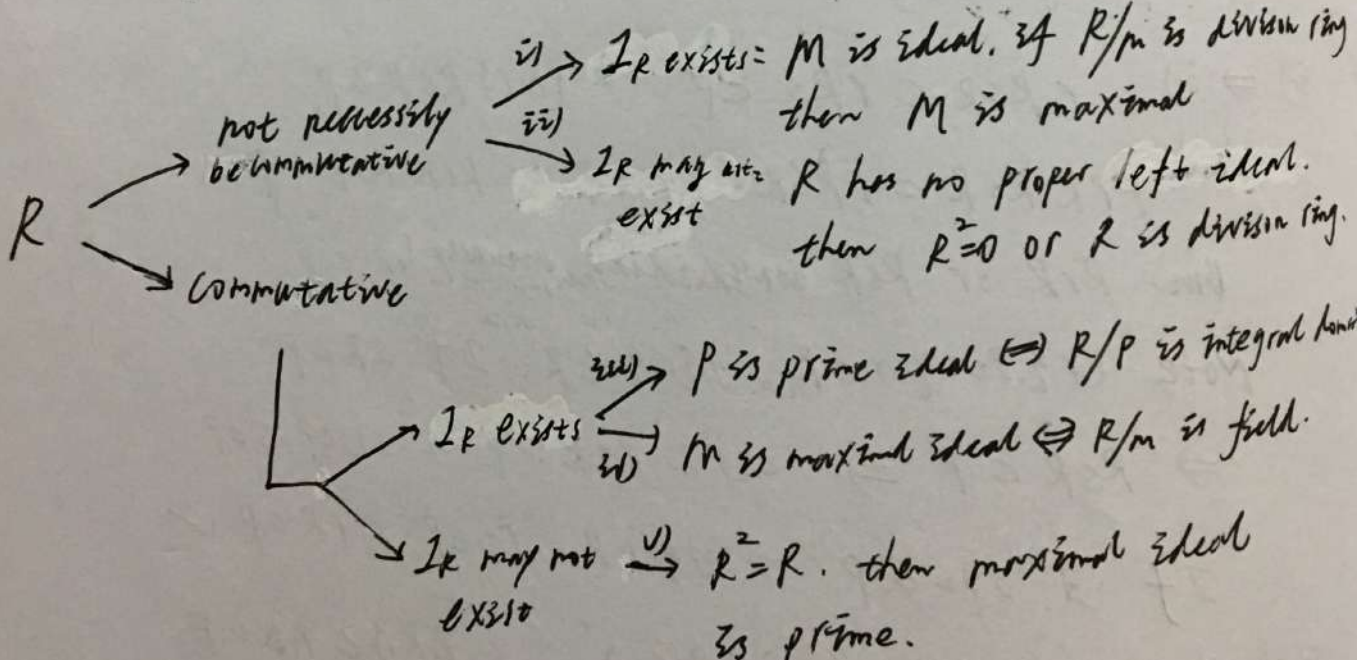
RU, RV are ideals $\therefore RU \subset P$ or $RV \subset P$.

choose $r_1 \in R-P \Rightarrow \forall u \in U$, $u \in P$ $\therefore U \subset P$!

Theorem. $R \neq \{0\}$. with 1_R. Maximal [left] ideals exist, containing every [left] ideals.

pf: Apply Zorn's lemma. $S = \{C \mid C$ is ideal in $R\}$. with "$\subseteq$" set theoretic inclusion. Check $\bigcup_{C \in \mathcal{C}} C$ is ideal and is upper bound of chain!

2.



pf: i) If N is ideal, st $M \subsetneq N$, pick $a \in N-M$

⇒ $a+M$ has inverse $b+m$ ⇒ $(a+m)(b+m) = ab+m = 1_R+m$

→ $1_R - ab \in M$ $\therefore \exists c \in m \subset N$ $1_R = ab+c$, $a \in N$ $\therefore ab \in N$.

$\therefore 1_R \subset N \quad \therefore N = R \quad \therefore M$ is maximal!

Cor. R is commutative with 1_R. M is maximal ideal iff $\forall r \in R-M, \exists x \in R$, s.t. $1_R - rx \in M$

Pf: ($\Rightarrow$) $(r)+M \supseteq M \quad \therefore (r)+M = R \quad \therefore \exists x \in R, m \in M$

s.t. $-rx + 1_R = m \in M$

($\Leftarrow$) Prove $(r)+M = R$ Note that $1_R = rx + m$.

$\Rightarrow \forall r' \in R. \quad r' \cdot 1_R = r'rx + r'm \in (r)+M.$

$\therefore R \subset (r)+M \subset R \quad \therefore (r)+M = R.$

ii) $[a \mid Ra = 0]$ is a left ideal. $\therefore$ It's $[0]$ or R.

If $[a \mid Ra = 0] = R \Rightarrow R^2 = [0]$. If $[a \mid Ra = 0] = [0]$

$[a \mid ab = 0, a \in R] = I_b$ is a left ideal. Since $[b \mid Rb = 0] = [0]$.

$\therefore I_b = [0]. \quad \therefore \forall b \in R$, s.t. has no zero divisor!

$\therefore Rb = R$. $\exists e$, s.t. $eb = b$. then

$xeb = xb. \ \forall x \in R \Rightarrow xe = x. \quad xey = xy. \ \forall y \in R.$

$\therefore ey = y \quad \therefore e$ is L-R identity $\Rightarrow \exists a$, s.t. $ab = e$.

$\therefore R$ is division ring.

→ Collect the target elements to an ideal.

iii) ($\Rightarrow$) $(a+p)(b+p) = p = ab+p \ (\in) \ ab \in p \ (\in) \ a \in p$ or $b \in p$.

($\Leftarrow$) $ab \in p \ (\in) \ a+p \in p$ or $b+p \in p$.

iv) ($\Leftarrow$) Done at i) ($\Rightarrow$) By cor. of i)

Remark: R is field $(\in)$ R has no proper ideal.

$(\in)$ $R \xrightarrow{f} S$, f is mono-

v) M is maximal $\Rightarrow a \in R-M$, $(a)+M=R$

If $pq \in M$. $p \notin M$. $q \notin M$. $\Rightarrow (p)+M=(q)+M=R$

$\therefore ((p)+M)((q)+M)=R^2=R=(p)(q)+M$

$\subset (pq)+M=M$ $\therefore R=M$. contradict!

3. (Prime Avoidance Lemma):

R commutative with 1_R. A is ideal in R.

st $A \subset \bigcup_1^n P_i$. P_i is prime ideal $\Rightarrow A \subset P_k$. some k.

Pf: By contraposition:

If $\forall 1 \le k \le n$. $\exists a_k \in A$. st. $a_k \notin P_k$.

we have $a_k \in \bigcup_{i \neq k}^n P_i$.

since $a_1 + \prod_{i=2}^n a_k \in A$. but $a_1 + \prod_{i=2}^n a_k \notin \bigcup_1^n P_k$

Otherwise. $a_1 + \prod_{i=2}^n a_k \in P_t$. for some t.

but $[a_k]_2^n \subseteq P_t$. except a_t. Contradiction!

4. A set consisting of 0 and all zero divisors in commutative R with 1_R contains at least 1 prime ideal

Pf: Let Z be the set $\Rightarrow R/Z$ is close.

$S = \{I \mid I \subseteq Z. I \lhd R\}$. Use Zorn's Lemma.

$\exists$ maximal ideal M in Z. Claim: M is prime.

$AB \subset M$. if $A \notin M$. $B \notin M$. then

$A+M$. $B+M \cap R/Z \neq Q$. both ideals containing M

Date.
No.

$\Rightarrow \exists a+p_1 \in (A+M)\cap(R/\sim)$, $\exists b+p_2 \in (A+M)\cap(R/\sim)$

$\therefore (a+p_1)(b+p_2) = p_1(b+p_2)+ap_2+\underline{ab} \in M$. contradict!

Remark: ✡: R commutative with 1_R. then

i) R has unique prime ideal ⇔ iii) R has minimal ideal containing all zero divisors. And nonunit are zero divisors

⇕

ii) every nonunit is nilpotent

pf: i) ⇒ iii) The maximal ideal is prime

$\because R$ is local ring: nonunits of R forms an ideal

$\because$ nilpotent elements forms an ideal too

$\therefore$ Nilpotent ⇔ nonunit.

iii) ⇒ i): The minimal ideal is maximum. ⇒ Unique!

ii) ⇒ iii) Note that 对 P is prime ideal.

then 对 r is nilpotent. $\Rightarrow r \in P$. since $r^n = 0 \in P$.

$\therefore r \in P$. then every prime ideal contains all nilpotent

But all nilpotent forms a prime ideal $\therefore$ The minimal prime ideal consists of all nilpotent. But every nonunit is nilpotent. so zero divisor □

② Chinese Remainder Theorem:

$\{A_i\}_1^n$ is family of ideals of R. s.t. $A_i+A_j=R$.

$R^2+A_i=R$. $\forall i,j$. 对 best R. then $\exists b \equiv b_i (A_i)$

And b is unique determind up to modulo $\bigcap_1^n A_i$

pf: Lemma. A,B are ideals. then $AB \subset A\cap B$.

pf: $AB \subset A$. $AB \subset B$. by A,B ideal. $\Rightarrow AB \subset A\cap B$.

Then since $(A_1+A_2)(A_1+A_3)=R^2=A_1+A_2A_3 \subset A_1+A_2\cap A_3$

$\therefore R^2+A_1 \subset A_1+A_2\cap A_3 \subset R \therefore A_1+A_2\cap A_3=R$.

generally, induct $R=A_1+\bigcap_2^k A_i$. $(A_1+\bigcap_2^k A_i)(A_1+A_{k+1})$

$+A_1=R \subset A_1+\bigcap_2^{k+1} A_i \subset R \Rightarrow R=A_1+\bigcap_{i\neq 1}^{n} A_i$.

$\therefore R=A_j+\bigcap_{i\neq j} A_i$. $\forall b_i \Rightarrow b_i=a_j+r_j$

Let $b=\sum_1^n r_j$. 对于 $b\equiv c \bmod A_j \Rightarrow b-c\in \bigcap_1^n A_i$

Cor. $R/\bigcap_1^n A_i \longrightarrow \prod_1^n R/A_i$ is mono-. If $A_i+A_j=R$.

$R^2+A_i=R$, then it's iso-

Pf: $R \longrightarrow \prod_1^n R/A_i$, kernel is $\bigcap_1^n A_i$ clearly

And by Chinese Reminder Theorem, it's epi!

③ ideal under homo-:

$R \xrightarrow{f} S$. ring homo-, then

i) $f^{-1}(I)$ is ideal. 对于 I is ideal. retaining the property of ideal. such as prime, contains kerf.

ii) $f(J)$ is an ideal, If J is an ideal and f is epi-, keep property

iii) principle ideal will retain whatever f or f^{-1}

④ $M^{n\times n}$ on unitary Ring R, denoted $S=M^{n\times n}(R)$

Then, J is an ideal in $S \Leftrightarrow J$ is $M^{n\times n}$ over an ideal I of R.

Pf: ($\Rightarrow$) J is an ideal in S. Let A be the set of all elements on entry $(1,1)$ of matrices in J. Claim: A is ideal of R.

Prove: If $M \in J \Rightarrow \forall a_1 E_{11}, a_2 E_{11} \in S$.

$(a_1 E_{11}) M (a_2 E_{11}) \in J \Rightarrow a_1 m_{11} a_2 \in A$

since $a_1 m_{11} a_2 E_{11} \in J$.

$\Rightarrow$ However, note that $E_{12} M E_{j1} = m_{ij} E_{11}$

$\therefore \forall m_{ij} \in A, \therefore M \in M_n(A)$.

If $N \in M_n(A)$, then $N = \sum n_{ij} E_{ij}$

Now prove $n_{ij} E_{ij} \in J$, $\forall i,j$. since $n_{ij} \in A$.

$\therefore \exists C = (c_{ij})$, $c_{11} = n_{ij}$, then by $C \in J$.

$\therefore E_{2i} C E_{1j} = c_{11} E_{ij} = n_{ij} E_{ij} \in J$.

$\therefore J = M_n(A)$

($\Leftarrow$) obvious. Test with Basis: $\{r E_{ij} \mid r \in R\}$.

Cor. If D is division Ring. Then $M_n(D)$ has no proper left ideal. But $M_n(D)$ isn't division ring. So $M_n(R)$ will not retain property of R

→ Criteria: R has no proper ideal with 1_R ($\Rightarrow$ Division R!

(3) Factorization in Commutative Ring

Relation: Integral Domain $\supsetneq$ UFD $\supsetneq$ PID $\supsetneq$ Euclidean Domain.

① Property of elements in unitary commutative R

ii) $a \mid b \Leftrightarrow (b) \subset (a)$. and u is unit $\Leftrightarrow (u) = R$

$\Leftrightarrow u \mid b. \ \forall b \in R.$

iii) If $d = gcd\{a_i\}_1^n$. s.t $d = \sum r_i a_i$

$\Leftrightarrow (d) = \sum_1^n (a_i)$

If R is integral domain

iii) p is prime $\Leftrightarrow (p)$ is prime. And prime element is irreducible

iv) c is irreducible $\Leftrightarrow (c)$ is maximal ideal in the set of principle ideals of R.

If R is UFD

v) prime element p coincide the irreducible element.

vi) $gcd\{a_i\}_1^n$ exists!

vii) Only finite principles ideal contain (c), $c \in R$.

If R is PID.

viii) Every proper ideal is product of $\prod_1^n P_i$

P_i is maximal ideal

ix) Def = primary ideal P = if $ab \in P$. and $a \notin P$. implies = $b^n \in P$. for some n

Then P is primary $\Leftrightarrow P = (p^n)$. p is prime or 0

Date.
No.

X) $\tilde{\prod}_1 P_i = \hat{\bigcap}_1 P_i$. $P_i = (p_i^{n_i})$, Then $\forall$ proper ideal is intersection of primary ideal in PID

Xi) gcd $(a_i)_1^n$ exists. with form $\sum_1^n r_i a_i$ (PIR ∨)

If R is Euclid Ring.

Xii) a is unit $\Leftrightarrow \varphi(a) = \varphi(1_R)$

pf: Viii) $= (a) = (\tilde{\prod}_1 p_i^{n_i})$. Lemma. If R is unitary and commutative. then $(ab) = (a)(b)$

prove: $(a)(b) \subseteq (ab)$ by commutative

And $\forall\ rab \in (ab) \Rightarrow ra \cdot 1_R b \in (a)(b)$

$\therefore (ab) = (a)(b)$

$\Rightarrow (a) = \hat{\prod}_1 (p_i)^{n_i}$. (p_i) is prime

iX) If $P = (p)$. $P = \hat{\prod}_1 p_i^{n_i}$, $n \geq 2$,

then $\tilde{\prod}_1^{n_1} p_i^{n_i} \cdot p_{n'}^{n_{n'}} \in (p)$. $\tilde{\prod}_1^{n_1} p_i^{n_i} \notin (p)$. $(p_{n'}^{n_{n'}}) \notin (p)$

Contradiction! $\therefore n \leq 1$. $P = P^n$.

X) $\pi P_i = (\tilde{\prod}_1 p_i^{n_i})$ 1') $\tilde{\prod}_1 p_i \subseteq \hat{\bigcap}_1 p_i$

$\forall\ a \in \hat{\bigcap}_1 p_i$. $(a) \subseteq \hat{\bigcap}_1 p_i \therefore (a) \subseteq p_i$. $\forall i$

$\therefore p_i^{n_i} \mid a$, $\forall i$ $\therefore \hat{\prod}_1 p_i^{n_i} \mid a \Rightarrow a \in (\pi p_i^{n_i})$

$\therefore \pi p_i = (\tilde{\prod}_1 p_i^{n_i}) = \hat{\bigcap}_1 p_i$.

X) $\langle a_1, a_2 \cdots, a_n \rangle = \langle d \rangle$ by PID.

$\Rightarrow (a_i) \subseteq (d) \Rightarrow d \mid a_i$. But

by $d = \sum r_i a_i$, then d is gcd$\{a_i\}$.

Xii) $\varphi(1_R) = \varphi(a \cdot a^{-1}) \geq \varphi(a)$ ($\Leftarrow$))

$= \varphi(a \cdot 1_R) \geq \varphi(1_R)$

($\Leftarrow$) $1_R = qa + r$. if $r \neq 0$

$\Rightarrow \varphi(a) = \varphi(1_R) > \varphi(r)$

$= \varphi(r \cdot 1_R) \geq \varphi(1_R)$. contradiction!

② Main Theorem:

i) PID is UFD ii) Euclid Ring is PIR. with id.

pf: i) Lemma: R is PIR, then: $(a_1) \subset (a_2) \cdots \subset (a_n) \cdots$ is chain of ideal. then for some n. $(a_n) = (a_k)$. $k \geq n$

pf: Actually. $\bigcup_{i=1} (a_i)$ is an ideal. check it!

$\therefore \bigcup_{i=1} (a_i) = (a) \Rightarrow a \in (a_n)$, for some n.

$\Rightarrow (a) \subseteq (a_n) \subseteq (a_k) \subseteq (a)$, $k \geq n$.

Now. We get ideal from Vii), If a is infinite product of irred. nonunits. $\exists a_1$.

$a = x_a a_1$. x_a is an irreducible element. So

a_1 is also infinite product of irred. nonunits.

And $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \cdots$ or x_a is unit, contradiction!

$\Rightarrow$ By Induction: $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \cdots$

Then contradict with Lemma!

$\therefore$ $\forall$ element in R is finite product of irreducible element.

If $a = \prod_1^n a_i = \prod_1^t b_i$. By Induction! since $\langle a_i \rangle, \langle b_i \rangle$ prime!

(2) I is an ideal in R. $S = \{\varphi(a) \mid a \neq 0\}$.

$\exists$ minimal elem: $\varphi(a)$. If $\forall b \in I$, $b = qa + r$.

$r \neq 0$, then $r \in I$, but $\varphi(r) < \varphi(a)$, contradict!

$\therefore$ $Ra = (a) = I$.

Since R is trivial ideal $\therefore R = (b) = Rb$.

$\therefore$ $b = eb$. $\Rightarrow \forall x \in R$, $x = yb$. $\therefore xe = ybe$

$= yb = x$. $\therefore e$ is id!

(3) Criterion of UFD.

Integral Domain is UFD $\Leftrightarrow$ every nonzero prime ideal contains a nonzero principle prime ideal.

Pf: ($\Rightarrow$) P is a prime ideal $\therefore ab \in P$. $a \in P$ or $b \in P$

$\therefore$ if $a \in P$. $a = \pi p_i^{n_i}$. $\exists p_k \in P$. p_k is prim $\therefore (p_k) \subset P$.

($\Leftarrow$) By localization.

(4) Ring of Quotients and Localization.

We suppose R is commutative following.

① Propert of $S^{-1}R = R \times S$

i) it has identity and retains commutation.

ii) If R is integral domain. S contains non-zero elements. then $S^{-1}R$ is integral domain

If S contains all nonzero element $\Rightarrow S^{-1}R$ is field.

② An important map: $\varphi_s : R \longrightarrow S^{-1}R$, $r \longmapsto rs/s$ $\forall s \in S$. check it's homo.

i) If S contains no zero divisors, φ_s is mono-

ii) If S consists of units, then φ_s is iso-

Remark: i) R is integral domain. Then it can embed into field.

ii) The complete ring of finite ring R $S^{-1}R \cong R$. since all elements in R are either zero divisors or units

iii) I is an ideal in R, then $I \subseteq \varphi_s^{-1}(S^{-1}I)$, (which means $r/s \in S^{-1}I$. r may not be in I) Note that $\varphi_s(I) = Is/s \subseteq S^{-1}I$!

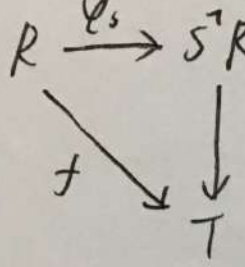
iv) Every ideal in $S^{-1}R$ is of form $S^{-1}I$.

I is an ideal in R.

v) If P is prime ideal, $S \cap P = \emptyset$, then $S^{-1}P$ is prime ideal in $S^{-1}R$, $\varphi_S^{-1}(S^{-1}P) = P$.

(Lemma: $S^{-1}I = S^{-1}R \iff I \cap R \neq \emptyset$)

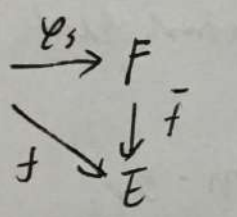
(3) Universal property of Ring of fraction



If f satisfies $\forall r \in R$, $f(r)$ is unit then $\exists! \bar{f}$, s.t. $\bar{f}\varphi_S = f$.
And $(\varphi_S, S^{-1}R)$ is universal object in category $C = (f, T)$

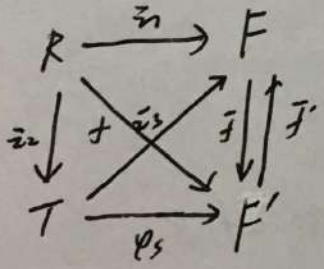
Pf: Def $\bar{f}(r/s) = f(r)\,\overrightarrow{f(s)}$

Cor. i)



F is field of R. f is mono- and E is field $\Rightarrow \exists! \bar{f}$.
s.t. $\bar{f}|_R = f$. $\exists F_1 \cong F$. $E_1 \cong E$.
$R \subseteq F_1 \subseteq E_1$ (By φ_S. f. $\bar{f}$ are all mono-!)

ii)



If R, T are integral domain. F is quotient field of R. and $R \subset T \subset F$, then the quotient field of $T = F' \cong F$

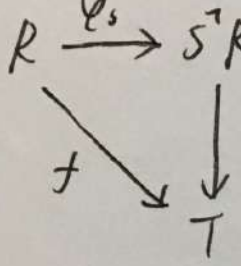
Pf: By i) i_3 is mono- $\therefore \bar{f}'$ is mono-, $F' \subseteq F$
$f = \varphi_S i_2$, mono- $\therefore \bar{f}$ is mono-, $F \subseteq F'$
$\Rightarrow F \cong F'$ by Bernstein Theorem.

Remark: Special Case: $R \cong T$, then $R \xrightarrow{g} T$ can be extended to $\bar{g}: F \to F'$, iso-.

v) If P is prime ideal, $S \cap P = \emptyset$, then $S^{-1}P$ is prime ideal in $S^{-1}R$, $\varphi_S^{-1}(S^{-1}P) = P$.

(Lemma: $S^{-1}I = S^{-1}R \iff I \cap R \neq \emptyset$)

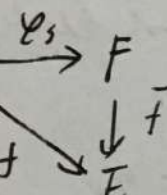
(3) Universal property of Ring of fraction



If f sastisfies $\forall r \in R$, $f(r)$ is unit then $\exists! \bar{f}$, s.t. $\bar{f}\varphi_S = f$.
And $(\varphi_S, S^{-1}R)$ is universal object in (ategory $C = (f, T)$

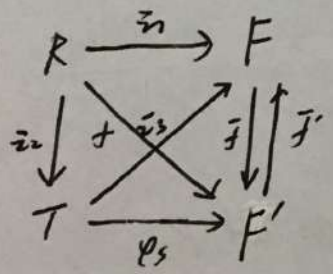
Pf: Def $\bar{f}(r/s) = f(r) f^{-1}(s)$

Cor. i)



F is field of R. f is mono- and E is field $\Rightarrow \exists! \bar{f}$.
s.t. $\bar{f}|_R = f$. $\exists F_1 \cong F$. $E_1 \cong E$.
$R \subseteq F_1 \subseteq E_1$ (By φ_S. f. $\bar{f}$ are all mono-!)

ii)



If R.T are integral domain.
F is quotient field of R.
and $R \subset T \subset F$. then the quotient field of $T = F' \cong F$

Pf: By i) i_3 is mono- $\therefore f'$ is mono-, $F' \subseteq F$
$f = \varphi_S i_2$. mono- $\therefore \bar{f}$ is mono-, $F \subseteq F'$
$\Rightarrow F \cong F'$ by Berstein Theorem.

Remark: Special Case: $R \cong T$. then $R \xrightarrow{g} T$ can be extended to $\bar{g}: F \to F'$. iso-.

Date.
No.

pf: i) ⇔ ii) ⇔ iii) obvious! since $I \neq R$. ⇔ I doesn't contain unit. And if a is nonunit ⇒ $(a) \subset$ Maximal ideal.

iv) ⇒ i) Suppose P, Q are maximal ideal.

Bwo $P \neq Q$. ∴ $\exists p \in P$. s.t. $p \notin Q$. ∴ $(p) + Q = R$.

∴ $\exists p' \in (p)$. and nonunit $q \in Q$. since $Q \neq R$.

s.t. $p' + q = 1_R$ ∴ p' is unit ⇒ $p' \in (p) \subset P$. ∴ $P = R$!

i) ⇒ iv) Nonunits form an ideal. If r, s are both nonunits. then 1_R is nonunit. contradiction!

Some conclusions of Local Ring:

1. Homo-image of Local Ring.

pf: since the maximal ideal M contains $\ker f$ ⇒ And the ideal containing kerf is one to one response to the ideal in $f(R)$ ∴ $f(R)$ is Local Ring!

2. M is maximal ideal in commutative unitary ring R. for some n. R/M^n is local ring.

pf: the ideal in R/M^n is one to one correspondense to the ideal containing M^n in R. ∴ The maximal ideal P is also prime in R/M^n. and. $M^n \subset P$. ⇒ $m^n \in M^n \subset P$ ∴ $m \in P$. $\forall m \in M$.

∴ $M \subset P$. ∴ $P = M$. Then P is unique

(5) Ring of Polynomial

① Definition:

For $R[x]$ = just def words: $\{(a_1, a_2 \cdots a_n \cdots) \mid a_i \in R\}$ with addition and multiplication. Or then induce a indeterminate "x". But essentially, define a map $f: N \longrightarrow R$. "i" is x^i. where $f(i)$ is coefficient.

$i \longmapsto r$

⇒ Then for $R[x_1, x_2 \cdots x_n]$: Similarly: def $f: N^n \to R$.

it extend one indeterminate to n indeterminates!

Basis maps $[x^{i_1} x^{i_2} \cdots x^{i_k}]$: Def by $x_{t_1}^{i_1} x_{t_2}^{i_2} \cdots x_{t_n}^{i_k}\left(\sum_1^k i_k e_{t_k}\right) = 1_R$.

$x_{t_1}^{i_1} \cdots x_{t_k}^{i_k}(u) = 0 \quad u \neq \sum i_k e_{t_k}$

sometimes, Ignore $[x_i]_1^n$. Consider S: a set.

Let $\varphi: S \longrightarrow N$. determine the power of indeterminates in S. Denote $[\varphi: S \to N] = N^S$

Then $R[S]$ is set of all maps $= [f: N^S \to R]$.

which determines the coefficient of φ.

② Universal Property of $R[x_1, x_2 \cdots x_n]$.

R, S are commutative

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ & \searrow^{i} & \uparrow \bar{\varphi} \\ & & R[x_1, x_2 \cdots x_n] \end{array}$$

Def: $\bar{\varphi}\left(\sum a_i x_1^{k_{i1}} \cdots x_n^{k_{in}}\right)$

$= \sum \varphi(a_i) s_1^{k_{i1}} \cdots s_n^{k_{in}}$

Generally, $R[S']$ satisfies it, too!

---

s.t. $\bar{\varphi}|_R = \varphi$, $\bar{\varphi}(x_i) = s_i$

(多项式函数用赋值!)

Cor. when $[S:\varphi(R)]$ is commutative, $\varphi(r)s_i = s_i\varphi(r)$.

Proposition 1. $R[x]/I[x] \cong (R/I)[x]$.

pf: $R[x] \xrightarrow{f} (R/I)[x]$. $\ker f = I[x]$.

Remark: i) I is maximal ideal $\not\Rightarrow$ $I[x]$ is
e.g. $R=\mathbb{Z}$, $I=\langle 2\rangle$, $I[x] \subseteq \langle 2, x\rangle$.

ii) So If R/I is Integral Domain, $(R/I)[x]$
need not be Integral Domain.

2. $F[x+1] \cong F[x]$
$\Rightarrow$ Then if F is field. (x) is maximal ideal.
But it's not unique. Since $F[x+1]/(x+1) \cong F[x]/(x)$.
Generally, $(x+k)$ is maximal ideal in $F[x]$

③ Ring of formal power series.

Property: i) f is unit in $R[[x]]$ ($\Leftrightarrow$ a_0 is unit in R.
ii) a_0 is irreducible $\Rightarrow$ $f=\sum_0 a_i x^i$ is irreducible in $R[[x]]$.
iii) If F is field, every nonzero element in $F[[x]]$
is the form $x^k u$. $u \in F[[x]]$ is an unit.
iv) F is field, then $F[[x]]$ is PID and local ring.
With ideal (x^k), $0 \le k \in \mathbb{Z}^+$. (x) is max!

pf: i) $g=\sum_0 b_i x^i \Rightarrow fg=1_k \Rightarrow b_0=a_0^{-1}$, $b_1=\frac{-a_1 a_0^{-1}}{a_0}$ .., $b_n=\cdots$; ...
(Inverse infinite seq $(b_i)_0^\infty$. by Induction! ii) By i)

iii) 设 $a \in F[[x]]$ and $a = a_0 + a_1x + \cdots a_nx^n \cdots$

then a_0 is unit $\Rightarrow$ a is unit.

设 $a = x^k \cdot a_k + x^{k+1}a_{k+1} - + x^n a_n + \cdots \Rightarrow a = x^k(a_k + a_{k+1}x + \cdots)$

$a_k + a_{k+1}x + a_{k+2}x^2 + \cdots$ is unit. $\therefore a = x^k \cdot u$.

iv) 设 $I \lhd F[[x]]$. $S = \{ v(f(x)) \mid f(x)$ is the minimal order of $f(x)\} \subseteq \mathbb{N}$, which is well-order

设 $0 \in S \Rightarrow \exists$ unit $u \in I \Rightarrow I = F[[x]]$.

设 $n_0 > 0$. $n_0 \in S$. it's minimal $\Rightarrow \forall f \in I$.

$\deg f \geq n_0 \Rightarrow f = x^{n_0}(a_0 + a_1x + \cdots a_nx^{n-n_0})$

$\therefore I \subseteq \langle x^{n_0} \rangle$. But $a_0 + a_1x + \cdots a_nx^{n-n_0} \cdots$ is unit

$\therefore \exists h \in F[[x]]$. s.t. $fh = x^{n_0} \in I$. $\therefore I = \langle x^{n_0} \rangle$

c) is the maximal unique ideal by the fact that $f \in F[[x]]$ is nonunit $\Leftrightarrow$ it's zero constant!

④ Factorization in Polynomial ring.

Main Theorem: D is UFD $\Rightarrow D[x]$ is UFD

Lemma. (where D is UFD. F is its quotient field.)

- Gauss Lemma.
- f and g associates in $D[x] \Leftrightarrow F[x]$
- f irreducible in $D[x] \Leftrightarrow F[x]$

$\Rightarrow$ Firstly. $D \to F$. $F[x]$ is Euclidean Domain

$f = c(f) f_1$. $c(f)$ is unit or $\tilde{\pi} c_i$ in D. c_i is irreducible.

$f_1 = \pi p_i^*$ in $F[x]$, p_i^* irreducible in $F[x]$.

and $p_i^* = \frac{b_i}{a_i} p_i$, p_i irreducible in $D[x]$ by Lemma.

$\Rightarrow \pi b_i = b$, $\pi a_i = a$. $\therefore a f_1 = b \pi p_i$

since f_1 is primitive in $D[x]$, and πp_i is.

$\Rightarrow a \backsim a c(f_1) = c(a f_1) = c(b \pi p_i) \backsim b$.

$\therefore f_1 \backsim \pi p_i$ in $D[x]$.

Uniqueness: By coefficients is associated:

$D[x] \longrightarrow F[x]$. Then polynomials are one to one correspondence!

Cor. By Induction: $D[x_1, x_2 \cdots x_n]$ is UFD!

Some conclusions:

1. R is commutative with 1_R. $f = \sum_0^n a_i x^i$ is unit in $R[x]$ ($\Leftrightarrow$) a_0 is unit and a_i ($1 \le i \le n$) are nilpotent in R.

pf: ($\Rightarrow$) $\exists\ g = \sum_0^m b_i x^i$, s.t. $fg = 1_R \Rightarrow$

$a_n b_m = 0$, $a_{n-1} b_m + a_n b_{m-1} = 0$

$\therefore a_{n-1} a_n b_m + a_n^2 b_{m-1} = 0 = a_n^2 b_{m-1} \cdots a_n^k b_{m-k+1} = 0$

$\therefore a_n^m b_0 = 0 \Rightarrow a_0 b_0 = 1_R \therefore a_n^m = 0$

Then induction on $\deg f$!

($\Leftarrow$) $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots a_n x^n$

$a_0^{-1} f(x) = 1_R + \underbrace{a_0^{-1}(a_1 x + \cdots a_n x^n)}_{\text{nilpotent. Denote } b}$

$\Rightarrow (1+b)(1-b)(1+b^2)(1+b^{2^2})\cdots(1+b^{2^n}) = 1$.

$\therefore f(x)$ is const!

2. R is integral domain. $I \subsetneq R$. If $p(x)$ is monic polynomial which can't be factored in 2 polynomials in $(R/I)[x]$. Then it's irred. in $R[x]$.

pf: If $p(x) = a(x)b(x)$, non constant polynomials. $(R/I)[x] \cong R(x)/I(x)$. then $\overline{p(x)} = \overline{a(x)}\,\overline{b(x)}$. by $a(x)$, $b(x)$ is monic. $\therefore \overline{a(x)}$, $\overline{b(x)}$ isn't constant.

3. $f = \sum_0^n a_i x^i \in \mathbb{Z}[x]$ reducible. If for k, $0<k<n$ and some p: $p \nmid a_n$, a_k. $p \mid a_i$, $0 \le i \le k-1$. $p^2 \nmid a_0$ then f has a factor g, $\deg g \ge k$, irreducible in $\mathbb{Z}[x]$.

pf: $f = c(f) f_1$. $f_1 = g_1 h_1$ Suppose $g_1 = \sum_0^t b_i x^i$ $h_1 = \sum_0^s c_i x^i$. By $p \nmid a_n$, $a_k \Rightarrow p \nmid c(f)$

$p \mid c_0 b_0$, say b_0. $b_0 c_1 + b_1 c_0 = a_1 \Rightarrow p \mid b_1$.

By Induction: $p \mid b_i$. If $t \le k-1$, then $p \mid c(g_1)$. contradict with f_1 is primitive.

$\therefore t \ge k$. $\therefore b_k, b_s$ can't be divided by p.

$\therefore$ By Induction on degree: Since $\deg g < \deg f$ use hypotheses on g!

4. If D is integral domain. Then the elements of $\mathrm{Aut}\,D[x]$ is form: $x \longmapsto ax+b$, $a \neq 0$.

Pf: If $f(g(x)) = x$, $g(x) = \sum_0^n a_i x^i$, $n \geq 2$.

$\Rightarrow \deg f \deg g = 1$. $\therefore \deg f = \deg g = 1$

$\Rightarrow g(x) = ax+b$, $f(x) = cx+d$ $\therefore ac = 1$.

Appendix: Exercises

1. R commutative, $|R| > 1$. If $\forall I \lhd R$, $\bigcap_{I \lhd R} I \neq 0$. And nonzero nilpotent element doesn't exist

Then. $\exists$ nonzero element e s.t. $e = e^2$, $e \in \bigcap I$.

Pf: $\exists c \neq 0$, s.t. $c \in \bigcap I$. construct an ideal:

$Rc^2 \Rightarrow c \in Rc^2$, $\therefore \exists r \in R$. $c = rc^2$

let $e = rc \Rightarrow e^2 = rrc^2 = rc = e$. and $e \in \bigcap I$.

2. If R has finite ideals. for $f: R \to R$, epi

then $f \in \mathrm{Aut}\,R$.

Pf: $\because R/\ker f \cong R$. Suppose $R/\ker f$ has proper ideals:

$\{I_i/\ker f\}_1^n$. which correspond to the ideals of R. If $\ker f \neq 0$, then $\ker f, \{I_i\}_1^n$ are $n+1$ ideals!

3. (Wedderburn) Finite division ring is field.

Pf: If D is a finite division ring.

$\because C(D)$ is center of D $\therefore C(D)$ is field.

See D as the vector space over $C(D)$.

Suppose $D \cong C(D)^n$. since it's finite.

And $|C(D)| = q$ $\therefore |D| = q^n$.

$\forall \alpha \in D$, $G_\alpha = \{x \mid x\alpha = \alpha x, x \in D\}$.

$\Rightarrow C(D) \subset G_\alpha \subset D$ $\therefore |G_\alpha| = q^d$. $d \mid n$. If $d < n$:

$\therefore |D| = |C(D)| + \sum \frac{|D|}{|G_\alpha|} \Rightarrow q^n = q + \sum_{d \mid n} \frac{q^n - 1}{q^d - 1}$

$\therefore q^n - 1 = q - 1 + \sum_{d \mid n} \frac{q^n - 1}{q^d - 1}$

$\sim$ $0 \in D$!

引入分圆多项式: $\Phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - \alpha_i)$, 其中 α_i 为 $x^n - 1 = 0$ 的根.

且 $\alpha_i = \varepsilon^k$, $(k, n) = 1$, $\varepsilon = e^{\frac{2\pi i}{n}}$, 则其个数恰为 $\varphi(n)$

且具有性质 $\prod_{d \mid n} \Phi_d(x) = x^n - 1$, Euler 引理 ($\sum_{d \mid n} \varphi(d) = n$)

Note that $\Phi_n(x) \nmid x^d - 1$, if $d < n$

$\therefore \Phi_n(q) \mid q^n - 1$ and $\frac{q^n - 1}{q^d - 1}$ $\therefore \Phi_n(q) \mid q - 1$

$\Rightarrow$ However. $0, 1 \in C$ $\therefore |C| = q \geq 2$.

$\Rightarrow |q - \varepsilon_i| \geq |q| - |\varepsilon_i| = q - 1 \geq 2 - 1 = 1$

$\therefore |\Phi_n(q)| > q - 1$, Contradict!

4. R is commutative. M is the maximal ideal.
then R/M is field $\Leftrightarrow \forall a \in R$, $a \notin M$, then $a^2 \notin M$.

Pf: When R has id. It's trivial!

($\Rightarrow$). If $\exists a \in R$, $a \notin M$, $a^2 \in M$.
then $\overline{a^2} = 0 = (\bar{a})^2 \therefore \bar{a} = 0$. Contradict!

($\Leftarrow$) Note that $(a)+M \supsetneq M$. if $a \notin M$.
By $a^2 = a \cdot a + 0 \in (a)+M$. $a^2 \notin M$.
$\therefore (a)+M = R$. $\Rightarrow (a+M) \cdot R/M$
$= ((a)+M)/M = R/M$
$\therefore \bar{a} \cdot \bar{a}^{-1} = \bar{1}_R$

5. If R contains finite ideals, R is integral domain. then R is field.

Pf: Note $\{Ra^k\}$ is set of ideals of R.
$\Rightarrow \exists\ Ra^k = Ra^l$, since ideals are finite. st. $k<l$.
$\Rightarrow \exists\ b$. st. $1_R a^k = b a^l \Rightarrow 1_R = b a^{l-k}$
$\therefore \forall a \in R$, a has an inverse.

6. (Kaplansky) If $a \in$ unitary ring R. having more than one right inverse, then it has infinite inverses.

Pf: $\{x_i\}_1^n$ is set of right inverses of a. $\{1-x_2 a+x_1\}_{i=1}^n$
~~is set of distinctive elements, by $1-x_i a+x_1 = 1-x_j a+x_1$~~

$\Rightarrow x_j a = x_i a \quad \therefore x_j = x_i$. And $a(1 - x_i a + x_1) = 1$.

对 $n < \infty$, $\exists i$, s.t. $1 - x_i a + x_1 = x_1$, since $[x_i]_1^n = [1 - x_i a + x_1]_1^n$

Then $1 = x_i a \quad \therefore x_j = x_i$. $\forall j \neq i$, $\therefore n = 1$. contradict!

Modules.

(1) Elementary:

1. A decomposition of unitary R-module:

$\exists B, C$, st. B is unitary, RC is 0. $A \cong B \oplus C$

pf: $B = \{1_R a \mid a \in A\}$. $C = \{a \mid 1_R a = 0\}$

$\forall a \in A$, $a = a - 1_R a + 1_R a$.

2. A criterion of mono and epi

$f: A \to B$. R-module homo.

i) f is mono $\Leftrightarrow \forall g, h: D \to A$. $\forall D$

对 $fg = fh$, then $g = h$

ii) f is epi $\Leftrightarrow \forall g, h: B \to C$. $\forall C$.

对 $gf = hf$, then $g = h$.

pf: i) $\Leftrightarrow \ker f = 0 \Leftrightarrow \ker f \xrightarrow{f'} A$, $f' = 0$

$\therefore$ let $h = 0$, $D = \ker f$

ii) $\Leftrightarrow B/f(A) = 0 \Leftrightarrow B \xrightarrow{g} B/f(A)$, $g = 0$.

3. Five Lemma.

$$\begin{array}{ccccccccc} A_1 & \longrightarrow & A_2 & \longrightarrow & A_3 & \longrightarrow & A_4 & \longrightarrow & A_5 \quad (\text{Exact row}) \\ \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5} \\ B_1 & \longrightarrow & B_2 & \longrightarrow & B_3 & \longrightarrow & B_4 & \longrightarrow & B_5 \quad (\text{Exact row}) \end{array}$$

i) α_3 is mono- $(\Leftarrow)$ α_2, α_4 are mono-, α_1 is epi-

ii) α_3 is epi- $\Leftrightarrow$ α_2, α_4 are epi-, α_5 is mono-

4. Compose the short exact row: $0 \to A \to B \xrightarrow{f} C \to 0$

$0 \to C \xrightarrow{g} D \to E \to 0$ are exact rows, then:

$0 \to A \to B \xrightarrow{gf} D \to E \to 0$ is exact, too!

(2) Free module and Vector space

① Criterion of free module.

1. In category of unitary R-modules,

F is free $(\Leftarrow)$ F has basis $(\Rightarrow)$ $F \underset{\text{def}}{\cong} \sum Ra \cong \sum R$.

$(\Rightarrow)$ F satisfies property of free object on set of basis.

Cor. $\forall$ unitary module is homo-image of free module.

2. In category of all left R-modules. (R is arbitrary)

F is free module on X $\Leftrightarrow$ F is free object on X in the category of left R-modules.

⇒ **Theorem**: we can find free module on any set X and arbitrary ring R

Pf: Lemma. $\{X_i\}_{i\in I}$ collection of disjoint sets. F_i is free on X_i. $X=\cup X_i$. $F=\Sigma F_i$. def: $\iota: X\to F$. by $\iota_i: X_i\to F_i$. $F_i \xrightarrow{\phi_i} F$. $\iota=\phi_i\iota_i$.

Then F is free on X.

Pf: $\cup X_i \xrightarrow{\iota} \Sigma F_i$, $\iota \downarrow \bar{f}$, $f: \cup X_i \to A$

suppose $X_i=\{x_{ik}\}$

$\Rightarrow \bar{f}(\sum_{i=1}\sum_{k} r_{ik}x_{ik})$

$= \sum_i \sum_k r_{ik} f(x_{ik})$

1) If R has identity:

give abelian grop Z trivial R-module struc.

$\Rightarrow R\oplus Z$ is R-module. with $r(r',m)=(rr',0)$

$X_t=\{t\}$. Def: $X_t \xrightarrow{\iota} R\oplus Z$, $\iota(t)=(1_R,1)$

Then $R\oplus Z$ is free module over X_t. by

$X_t \xrightarrow{\iota} R\oplus Z$, $\iota \downarrow \bar{f}$, $f: X_t \to A$

$A \cong B\oplus C$. s.t. $RC=0$. B is unitary.

if $f(t)=b+c$, def: $\bar{f}(r,m)$

$= rb+mc$. since $(r,m)=r(1_R,1)+m(1_R,1)$

Then let $X=\cup X_t$. with $\Sigma R\oplus Z$.

2) If R has no id: $R \xrightarrow{\text{embed}} S$. with id.

char $S=0$. S is free R-module on $X_t=\{t\}$.

$\{t\} \xrightarrow{\iota} S$, $\iota \downarrow$, $f: \{t\} \to A=B\oplus C$

$f(t)=b+c$ $\iota(t)=(0,1)$, $f(r,m)$

$= rb+mc$. □

Property: If F has infinite basis X, then

F is invariant-dimension, which is $|X|$

Pf: 1) Every basis of F is infinite denote X and Y.

2) Ref: $k(Y)$ is family of finite sets of Y.

$\forall x \in F,\ x = \sum_1^n r_i y_i,\ y_i \in Y,\ \forall i.$

$\Rightarrow f: X \longrightarrow k(Y)$, $\Rightarrow f(x)$ is infinite.
$x \longmapsto \{y_i\}_1^n$. If $T \in k(Y)$, T is finite $\Rightarrow \vec{f}(T)$ finite

Ref: $g_T: \vec{f}(T) \longrightarrow T \times N \Rightarrow X \xrightarrow{\varphi} Inf \times N$, injective
$x_k \longmapsto (T, k)$ $x \mapsto g_T(x),\ x \in \vec{f}(T)$

② Vector Space:

Theorem: D is division ring $\Leftrightarrow$ Every unitary D-module is free.

pf: ($\Leftarrow$) $I \triangleleft D$, I is maximal left ideal. free D-module
$\therefore I$ is projective $\Rightarrow D \cong I \oplus I'$. $I' \triangleleft D$, so I' is!
$\Rightarrow D \cong \Sigma D \oplus \Sigma D = D^k$. $D/I \cong D^t$. D/I is simple
by I is maximal $\therefore I' \cong D \cong D/I$ $\therefore I = 0$!

($\Rightarrow$) Vector space has basis! Which is the maximal linear independent set

③ Invariant dimension property of rings.

Lemma. R is unitary, F is free R-module, then

If $I \lhd R$, $\pi: F \to F/IF$, X is basis of F.

$\pi(X)$ is basis of $F/IF \Rightarrow |X| = |\pi(X)|$

Pf: check $\pi(X)$ is actually basis of F/IF.

$X \xrightarrow{\pi} \pi(X)$ is 1-1 ! By $\pi(X)$ is Basis!

(II)

Pro: S has invariant dimension property, $R \to S$ is epi- of unitary ring. So does R.

Pf: $R/I \cong S$. If X, Y are 2 basis of free R-module $\Rightarrow |\pi(X)| = |\pi(Y)| = |X| = |Y|$

Remark: Usually choose S is division ring.

If R is commutative unitary $\Rightarrow R^n \cong R^m \Leftrightarrow m = n$.

✡ Left-Ore Condition: If R has no zero divisor and satisfies $\forall r, s \in R$, $\exists a, b \in R$, st. $ar + bs = 0$ then: 对 $R \cong K \oplus L$, then $K = 0$ or $L = 0$

Pf: Let $r \in K$, $s \in L$. $\Rightarrow ar = -bs \in K \cap L = 0$

$\therefore \forall r \in K$, $r = 0$ or $\forall s \in L$, $s = 0$. $\Rightarrow K$ or $L = 0$!

$\Rightarrow$ If K has identity, then R has invariant dimension property.

Pf: Note that R^n keep the Lefe-ore condition.

$\exists m>n$. s.t. $R^n \cong R^m \cong R^n \oplus R^{m-n}$

$\Rightarrow R^{m-n}=0$ Generally $\exists R^n \cong R^n \oplus N$. $\exists N=0$

(3) Projective and Injective.

① Projective

construct $P \to F$!

Projective $\Leftrightarrow$ (P is projective), $\forall$ exact seq:

use universal: construct $X \to \square$

$0 \to A \to F \rightleftarrows P \to 0$. Split

free module is projective

$\exists$ free module F. s.t. $F \cong A \oplus P$.

Every module is homo-image of projective module!

$\Rightarrow$ **Property**: ΣP_i is projective $\Leftrightarrow$ every P_i is projective.

(use i_k and π_k relate ΣP_i with P_k!)

② Injective

Injective

(1) $\Leftrightarrow$ (J is injective). $\forall$ exact seq: $0 \to J \to B \to C \to 0$ is split exact. $\Leftrightarrow$ $\forall$ module B, s.t. $J \subset B$. we $C = B/J$ then J is direct summand of B.

(2) **Criteria**: R is unitary ring. R-module J is injective $\Leftrightarrow \forall L$ is left ideal of R, $\forall L \to J$ can be extend to $R \to J$.

(3) **property** → $\prod J_i$ is injective $\Leftrightarrow J_i$ is, $\forall i$

$\Leftrightarrow$ every R-module can embed into injective M!

Pf: (=) ($\Leftarrow$) $L \xrightarrow{c} R$, $L \to J$, $R \to J$ (dashed) — it's easy to see!

($\Leftarrow$) If $A \xrightarrow{f} B$, $A \to J$. By Zorn's Lemma.

Prove: $\exists\, C$, s.t. $\mathrm{Im} f \subset C \subset B$, $A \xrightarrow{f} C$, $C \to J$

C is maximal $\Rightarrow C = B$!

Construct left ideal: $b \in B - C$, $H = \{r \mid rb \in C\}$.

Remark: It's ($\Leftarrow$) $\forall\, L \trianglelefteq R$, $L \xrightarrow{g} J$, then $\exists\, a \in J$.

s.t. $g(r) = ra$. $\forall\, r \in L$.

(3) (*) Process:

i) Criteria of abelian group D:

D is divisible $\Leftrightarrow$ D is injective $\mathbb{Z}$-module

ii) Every abelian group can be embedded into divisible abelian group

Pf: $F \longrightarrow A$, F is free $\Rightarrow A \cong F/k \cong \Sigma\mathbb{Z}/k$

$F \cong \Sigma\mathbb{Z} \xrightarrow{i} \Sigma\mathbb{Q}$. $\Rightarrow i(F)/i(k) \cong F/k$.

$\therefore A \cong i(F)/i(k) \hookrightarrow \Sigma\mathbb{Q}/i(k)$

iii) J is divisible abelian group. R is unitary

$\Rightarrow \mathrm{Hom}_{\mathbb{Z}}(R, J)$ is injective left R-module

Pf: $\forall\, L \xrightarrow{f} \mathrm{Hom}_{\mathbb{Z}}(R, J)$, def $g: L \to J$

by $g(a) = [f(a)](1_R)$, extend $g \to \bar{g}$

Then def $\bar{f}: R \longrightarrow Hom_{\mathbb{Z}}(R,J)$. $\bar{f}(a)(x) = \bar{g}(xa)$

check $\bar{f}$ is well-def. R-module. $\bar{f}|_L = f$.

$\Rightarrow$ $A \xrightarrow{f} J$. by ii), $\bar{f}: Hom_{\mathbb{Z}}(R,A) \longrightarrow Hom_{\mathbb{Z}}(R,J)$

induced by $\bar{f}(g) = f \circ g$. $\bar{f}$ is mono-

$\therefore$ $A \cong Hom_R(R,A) \hookrightarrow Hom_{\mathbb{Z}}(R,A) \xrightarrow{\bar{f}} Hom_{\mathbb{Z}}(R,J)$

③ Conclusions:

1. Conditions on R are equivalent:

i) Every R-module is projective $\Leftrightarrow$ ii) Every R-module is injective.

$\Updownarrow$

iii) every short exact seq of R-module is split.

$\Rightarrow$ Vector space is both projective and injective.

2. Structure of divisible abelian group.

i) $D \cong D_t \oplus E$. E is torsion-free.

ii) $D_t \cong \sum \mathbb{Z}(p_i^{\infty})$. then $D_t \cong \sum \mathbb{Z}(p_i^{\infty})$ $\Rightarrow$ $D \cong \sum \mathbb{Z}(p_i^{\infty}) \oplus \sum \mathbb{Q}$.

iii) $E \cong \sum \mathbb{Q}$.

Pf: i) homo of divisible group is divisible $\Rightarrow$

$D \xrightarrow{\pi} D_t$ $\Rightarrow$ D_t is injective $\Rightarrow$ $D_t \subseteq D$ $\therefore$ $D \cong D_t \oplus E$.

ii) $px_1 = 0$, then $x_1 = px_2 \cdots x_n = px_{n+1}$ $\therefore$ $\forall x_i = \langle x_i \rangle \cong \mathbb{Z}(p^{\infty})$

iii) E is vector space over $\mathbb{Q}$.

3. Co-free — Dual def:

R-module homo: $\bar{f}$!

$F \xrightarrow{\iota} X$ ⇒ 对 $|X| \geq 2$. F doesn't exist.

$\bar{f}$ ↖ ↑ f A 对 $|X| = 1$. $F = \{0\}$.

Pf: i). suppose $\iota(0) = x_1$. choose f. st.

$f(0) = x_2$. $\alpha \in A$. ⇒ $\iota\bar{f}(\alpha) = \iota(0) = x_1$

$= f\iota(0) = x_2$. contradiction!

ii) 对 $|F| \geq 2$. ⇒ $F \xrightarrow{\iota} X$

$\bar{f}$ ↖ ↑ f F

$\iota(F) = X = \{x\}$.

$= f(F)$. But then

$\bar{f} = 0$ or id. contradict with unique!

(4) Hom and Dual.

① Functor:

1. i) $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ is exact seq ⇔ ∀ R-module D.

$0 \to \mathrm{Hom}_R(D, A) \xrightarrow{\bar{\varphi}} \mathrm{Hom}_R(D, B) \xrightarrow{\bar{\psi}} \mathrm{Hom}_R(D, C)$ is exact

ii) $A \xrightarrow{\theta} B \xrightarrow{\xi} C \to 0$ is exact seq ⇔ ∀ R-module D

$0 \to \mathrm{Hom}_R(C, D) \xrightarrow{\bar{\xi}} \mathrm{Hom}_R(B, D) \xrightarrow{\bar{\theta}} \mathrm{Hom}_R(A, D)$ is exact.

Generally. i) $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ split exact seq

⇕

ii) $0 \to \mathrm{Hom}_R(C, D) \xrightarrow{\bar{\varphi}} \mathrm{Hom}_R(B, D) \xrightarrow{\bar{\psi}} \mathrm{Hom}_R(A, D) \to 0$

is split exact. for every R-module D.

iii) $0 \longrightarrow \mathrm{Hom}_R(D,A) \xrightarrow{\bar{\varphi}} \mathrm{Hom}_R(D,B) \xrightarrow{\bar{\psi}} \mathrm{Hom}_R(D,C) \longrightarrow 0$
is split exact seq for $\forall D$.

2. R is unitary ring $\Rightarrow A \cong \mathrm{Hom}_R(R,A)$

(By $f \longmapsto f(1_R) \longmapsto f_{f(1_R)}$, s.t. $f_{f(1_R)}(a) = af(1_R)$)

$A \cong \mathrm{Hom}_R(R,A) \xleftrightarrow{\text{Dual}} \mathrm{Hom}_R(A,R) = A^*$.

$\Rightarrow$ $A \xrightarrow{\varphi} C$, then induces: $C^* \cong \mathrm{Hom}_R(C,R) \xrightarrow{\bar{\varphi}} A^* \cong \mathrm{Hom}_R(A,R)$

or $\mathrm{Hom}_R(A,D) \xrightarrow{\bar{\varphi}} \mathrm{Hom}_R(L,D)$, $\mathrm{Hom}_R(D,A) \xrightarrow{\bar{\varphi}} \mathrm{Hom}_R(D,C)$

Property: i) $(A \oplus C)^* \cong A^* \oplus C^*$

ii) The exact seq of vector space induces an exact seq of dual-!

iii) F is free on X, if X is finite $\Rightarrow$ $F \cong F^*$, but if F free module over arbitrary ring, F^* need not be free!

Dual Double: i) $\exists\ \theta: A \longrightarrow A^{**}$ def by: $\theta(a)(f) = \langle a, f \rangle$, then if A is free $\Rightarrow$ θ is mono-, if A is finite-basis-free $\Rightarrow$ θ is iso-!

ii) $\theta: A \longrightarrow A^{**}$ is iso-, then call

A is reflective.

Remark: If P is finitely generated projective unitary R module, then P^* is, too. And P is reflective.

Pf: i) $\exists$ free module F, s.t. $F \cong P \oplus Q$.

Note if $F \to F^{**}$ is iso. $\Rightarrow P \to P^{**}$, iso.

Note that F is free so projective.

$\Rightarrow \exists$ Split exact seq:

$$\begin{array}{ccccccc} 0 & \to & N & \to & R^k & \to & F \to 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \to & N^{**} & \to & (R^k)^{**} & \to & F^{**} \to 0 \end{array}$$

$\because R^k \cong (R^k)^{**}$

$\Rightarrow F \cong F^{**}$.

ii) $F^* = (P \oplus Q)^* = P^* \oplus Q^* = \mathrm{Hom}_R(F, R)$

$\cong \mathrm{Hom}_R(R^n, R) \cong \Sigma \mathrm{Hom}_R(R, R) = R^n$

$\therefore P^*$ is direct summand of free module

iii)

$$\begin{array}{ccc} A & \xrightarrow{\theta_A} & A^{**} \\ f \downarrow & & \downarrow f^{**} \\ B & \xrightarrow{\theta_B} & B^{**} \end{array}$$

$\Rightarrow f^{**}$ induced by $f^*: B^* \to A^*$.

then the diagram is commutative.

Pf: $f^{**}(\theta_A(a))_{(b)} = \theta_A(a)(f^*(b))$

$= \langle a, f^*(b) \rangle$, $\forall b \in B^*$

$= \langle f(a), b \rangle$

$\theta_B \circ f(a)(b) = \langle f(a), b \rangle$

$= \langle a, f^*(b) \rangle$

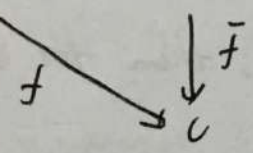
②

Projective (P) $\Leftrightarrow$ $\psi: B \to C$ is R-module epi., then $\bar{\psi}: \mathrm{Hom}_R(P,B) \to \mathrm{Hom}_R(P,C)$ is epi.

Injective (J) $\Leftrightarrow$ $\psi: B \to C$ is mono., then $\bar{\psi}: \mathrm{Hom}_R(C,P) \to \mathrm{Hom}_R(B,P)$ is mono.

(5) Tensor Product:

① Property: i) $A \times B \xrightarrow{\otimes} A \otimes_R B$

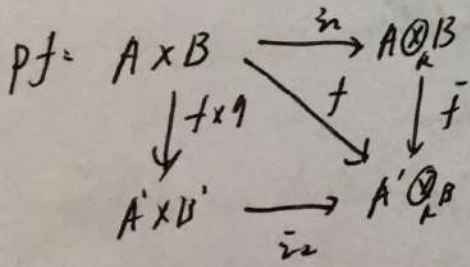


C is abelian group. $A \times_R B$ $\Rightarrow \exists$ unique $\bar{f}$.

$\Rightarrow$ Cor. $f: A \to A'$, $g: B \to B'$, then induce

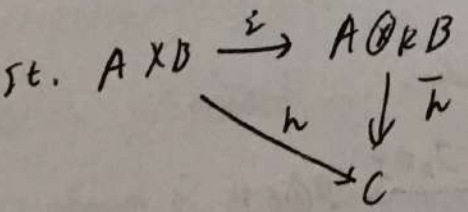
$f \otimes g: A \otimes_R B \to A' \otimes_R B'$

Pf:



$\bar{f} = f \otimes g$. check.

ii) If R is commutative, i.e. $r(a \otimes b) = ra \otimes b = a \otimes rb$), then $\forall$ C, R-module, ..., $\exists$ unique $\bar{h}$:



② Weak homo-:

$I, J \trianglelefteq R$. commutative. $\Rightarrow R/I \otimes_R R/J \cong R/I+J$.

Property:

- $A \otimes_R R \cong A$
- $A \otimes_R (B \otimes_S C) \cong (A \otimes_R B) \otimes_S C$
- $(\sum A_i) \otimes_R B \cong \sum (A_i \otimes_R B) \to S \otimes R^n \cong S^n$.
- $\mathrm{Hom}_S(A \otimes_R B, C) \cong \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$

$\cong \mathrm{Hom}_R(B, \mathrm{Hom}_S(A, C))$

③ Exact seq:

1. $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is exact seq. then for $\forall D_R$.

$D \otimes_R A \xrightarrow{1_D \otimes f} D \otimes_R B \xrightarrow{1_D \otimes g} D \otimes_R C \to 0$

$\Rightarrow$ Generally. If f is mono-. $1_D \otimes f$ need not be mono-

We induce flat module: D is a flat module.

If $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is exact seq. then

$0 \to D \otimes_R A \xrightarrow{1_D \otimes f} D \otimes_R B \xrightarrow{1_D \otimes g} D \otimes_R C \to 0$ is exact seq.

Pro. If D is projective unitary right R-module.

then D is flat module.

pf: only prove: $D \otimes_R A \xrightarrow{1_D \otimes f} D \otimes_R B$ is mono-

Note that: $\exists F$. free. $F \cong D \oplus D'$

$\therefore F \otimes A \cong (D \otimes A) \oplus (D' \otimes A)$

Date.
No.

$\because F \cong R^n \Rightarrow F \otimes A \cong \Sigma R \otimes_R A \cong A^n$.

$\therefore F \otimes_R A \longrightarrow F \otimes_R B \Leftrightarrow A^n \longrightarrow B^n$: injection.

$\therefore D \otimes_R A \xrightarrow{1_D \otimes f} D \otimes_R B$ is mono-!

Remark: If $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is split

, then latter holds. furthur. it's split.

By: $D \otimes B = D \otimes (A \oplus C) \cong (D \otimes A) \oplus (D \otimes C)$

④ With free module F.

F is free on $Y = \{y_j\}$. A is unitary right R-module

then $A \otimes F$ generated by $\{a \otimes y_i\}_{\substack{i \in I \\ a \in A}}$

$\Rightarrow$ Cor. $F_1 \otimes_R F_2$ is generated by $\{x_i \otimes y_j\}$

(b) Modules on PID

i) Free module F over PID. $E < F \Rightarrow E$ is free

→ Cor. F over PID is free $\Leftrightarrow$ F is projective.

ii) Submodules of finitely generated module over PID are finitely generated.

iii) Finitely generated torsion-free module over PID is free

Construct submodule of free module by map!

Criteria of PID: R is commutative unitary. If every submodule of every free R-module is free $\Rightarrow$ R is PID.

② Decomposition of finitely generated modules over PID

Step 1: separate torsion and torsion-free

$$A \cong A_t \oplus F, \quad F \text{ is free.}$$

Step 2. $A_t \cong \sum A(p)$

Step 3. $A(p) \cong \sum_{a_i \in A(p)} Ra_i$. By: $Ra_i \cong R/G_{a_i} = R/(r_{a_i})$

$$\therefore A(p) \cong \sum R/(r_{a_i}), \quad r_{a_i} = p^{a_i}$$

Step 4. $A \cong \sum R/(p_i^{k_i}) \oplus F$.

$$\cong \sum R/(r_i) \oplus F. \quad \text{s.t. } r_1 | r_2 \cdots | r_n.$$

By: $R/(r) \cong \sum R/(p_i^{k_i})$, 对 $r = u \prod p_i^{k_i}$.

Remark: We can also use the annihilator:

记 $\operatorname{ann} A = \{r \in R \mid rA = 0\}$, $M(a) = \{x \in M \mid ax = 0\}$.

$\Rightarrow$ Lemma. i) $\operatorname{ann} A$ is an ideal.

ii) $M((a,b)) = M(a) \cap M(b)$

iii) $M(ab) = M(a) \oplus M(b)$, 对 $(a,b) = 1$.

iv) $\operatorname{ann} M = \bigcap_{x \in M} \operatorname{ann} x = (a_m) \cdot (a_m)$

v) monotonicity

vi) $M(a_m) = M = \sum M(p_i^{k_i})$ 对 $a = u \prod p_i^{k_i}$.

② Decomposition of finitely generated modules over PID

Step 1: separate torsion and torsion-free

$$A \cong A_t \oplus F, \quad F \text{ is free.}$$

Step 2. $A_t \cong \sum A(p)$

Step 3. $A(p) \cong \sum_{a_i \in A(p)} Ra_i$. By: $Ra_i \cong R/\mathrm{Ann}\, a_i = R/(r_{a_i})$

$$\therefore A(p) \cong \sum R/(r_{a_i}), \quad r_{a_i} = p^{a_i}$$

Step 4. $A \cong \sum R/(p_i^{k_i}) \oplus F$.

$$\cong \sum R/(r_i) \oplus F, \text{ s.t. } r_1 \mid r_2 \cdots \mid r_n.$$

By: $R/(r) \cong \sum R/(p_i^{k_i})$, 对 $r = u\prod p_i^{k_i}$.

Remark: We can also use the annihilator:

记 $\mathrm{ann}\, A = \{r \in R \mid rA = 0\}$, $M(a) = \{x \in M \mid ax = 0\}$.

$\Rightarrow$ Lemma. 对 $\mathrm{ann}\, A$ 是 an ideal.

对 $M(ab) = M(a) \cap M(b)$

若对 $M(ab) = M(a) \oplus M(b)$, 对 $(a,b) = 1$.

对 $\mathrm{ann}\, M = \bigcap_{x \in M} \mathrm{ann}\, x = (a_m), (a_m)$

若 monic and

对 $M(a_m) = M = \sum M(p_i^{k_i})$, 对 $a = u\prod p_i^{k_i}$.

② Theorem. (Another projection)

Ref: $A \otimes_k B \xrightarrow{\alpha} B \otimes_k A$. check α is iso-

$\Rightarrow (A \otimes_k B) \otimes_k (A \otimes_k B) \xrightarrow{1_A \otimes \alpha \otimes 1_B} (A \otimes_k A) \otimes_k (B \otimes_k B)$

$\xrightarrow{\gamma_A \otimes \gamma_B} A \otimes_k B$. compose the homo-!

Fields

(1) Field extension:

① Transcendental extension:

Property: i) $\forall$ element in $k(x_1 \cdots x_n) - k$ is transcendental over k.

ii) $k(u) \cong k[x]$ (polynomials)

② Algebraic extension:

① A criterion: F is algebraic of $k \iff$ $\forall$ intermediate field E with mono-: $\sigma: E \to E$. if $\sigma|_k = id$. Then $\sigma \in Aut_E$

② Property: i) Finite extension is Algebraic

$\Rightarrow$ Cor. F is algebraic over k. E is algebraic over $F \Rightarrow$ then E is algebraic over k.

设 $u \in F$ 是 algebraic over k. $k \subseteq F$.

then $k[u] = k(u) \cong k[x]/(f)$, f 是 irreducible poly-. 使 $f(u)=0$. and $[k(u):k] = \deg f$

Pf: $\varphi: k[x] \longrightarrow k[u]$ epi-.
$g \longmapsto g(u)$

$\therefore \exists \ker\varphi = (f)$. by $k[x]$ 是 PID

$k[x]/(f) \cong k[u]$. which is integral domain

$\therefore (f)$ is prime. then irreducible and maximal

$\therefore k[u]$ 是 field contain $k \cup \{u\} \Rightarrow k(u)$!

Cor. If $k \subset F$. F 是 algebraic extension on k and E is intermediate integral domain. then E 是 field.

Pf: $\forall a \in E$. $k[a] = k(a) \subset E$. $\therefore a^{-1} \in E$!

② Extension 的 iso- of fields:

$\sigma: k \to L$. iso- of fields

- u, v are transcendental over k, L
- u 是 root of irred. f. v is root of σf

$\Rightarrow \sigma$ extend to $\tilde{\sigma}: k(u) \to L(v)$. 使 $\tilde{\sigma}(u) = v$

$\tilde{\sigma}$ 是 iso-

$\Rightarrow$ cor. $k(u) \cong k(v)$. $\Leftrightarrow u, v$ is root of the same irreducible polynomial.

③ Some conclusions:

1. $\bar{E}$ is set of all algebraic elements of F which is extension of k. $\Rightarrow \bar{E}$ is field.

Pf: $\forall u, v \in \bar{E}$. $k \subset k(u,v) \subset \bar{E} \therefore uv, u \cdot v \in \bar{E}$.

2. Dimension:

i) If u, v are algebraic over k of order m, n

$\Rightarrow [k(u,v):k] \leq mn$. Iff $(m,n)=1$. $\Rightarrow [k(u,v):k]=mn$.

ii) L, M are intermediate fields of $k \subset F$.

then $[LM:k]$ is finite $\Leftrightarrow [L:k], [M:k]$ are finite.

$\Rightarrow$ generally, $[LM:k]_{(finite. Assume)} \leq [L:k][M:k]$.

when $([L:k], [M:k])=1$. "$=$" hold

$\Rightarrow$ Moreover. If $[LM:k]=[L:k][M:k]$. then $L \cap M = k$. Converse holds if $[L:k]=2$.

Pf: i) $[k(u,v):k] = [k(u,v):k(u)][k(u):k]$

$= [k(u,v):k(v)][k(v):k] = n'm = m'n$

Note that $k(v) \supseteq k$. $\Rightarrow [k(v)(u), k(v)]$

$\leq [k(u):k] \Rightarrow n' \leq n$. $m' \leq m$

If $(m,n)=1 \Rightarrow m, n \mid [k(u,v):k]$.

$\therefore mn \mid [k(u,v):k] \therefore [k(u,v):k]=mn$.

(二)

2) If $[LM:k] \geq [L:k]$ or $[M:k]$.

(⇐) Note that if $\{u_i\}_1^n$ is basis of L/k.
$\{v_i\}_1^n$ is basis of $M/k \Rightarrow \{u_i v_j\}$
span LM/k. contains basis of LM/k.

$\therefore [LM:k] \leq [L:k][M:k]$

2) $L, M \geq k \therefore L \cap M \geq k$.

$\therefore [LM:k] = [LM:L \cap M][L \cap M:k]$

$\leq [L:L \cap M][M:L \cap M][L \cap M:k]$

$\therefore [L:k] \leq [L:L \cap M] \therefore L \cap M \leq k$

Conversely. By $[LM:k] \leq [L:k][M:k]$

if $[LM:k]/[M:k] = 1 \Rightarrow LM = M$.

$\therefore L \subset M \therefore L \cap M = L = k$. contradict!

(2) Fundamental Theorem

✡ A useful Lemma: $k \leq F$. $f \in k[x]$. if u is a root of f. $\sigma \in \mathrm{Aut}_k F$. then $\sigma(u)$ is also root of f.

Remark: Namely, $\forall \sigma \in \mathrm{Aut}_k(u)$ is the permutation of different roots partly. $\therefore |\mathrm{Aut}_k k(u)| \leq m$
m is the number of different roots.

Three Parts

i) Estimation:

① Lemma:

1. $F \supseteq k$. L, M are intermediate fields with $L \subset M$. $\Rightarrow [M:L] \geq [L':M']$

2. Or H, J are subgroups of $Aut_k F$ with $H < J \Rightarrow [J:H] \geq [H':J']$

(II)

ii) close fields:

1. $F \supseteq k$. $L \supset M$ are intermediate fields $H < J < Aut_k F$. then:

If M, H are close $\Rightarrow L, J$ are close and $[L:M] = [M':L']$, $[J:H] = [H':J']$

2. Cor. F is finitely Galois extension of k

$\Rightarrow$ all intermediate fields and all subgroups of $Aut_k F$ are close

iii) Stable:

1. If E is stable intermediate field of $k \subseteq F$. $H \triangleleft Aut_k F$. then $\bar{E}' \triangleleft Aut_k F$. H' is stable

2. F is Galois extension of k. E is stable intermediate field then $\bar{E}$ is Galois over k.

3. $k \subseteq F$. E is Galois intermediate algebraic field of $k \subseteq F$. then E is stable.

Remark: Actually. Galois algebraic intermediate field is seperable extension:

pf: If $u \in E$, $\exists f \in k[x]$. st $f(u)=0$. irr.

$\{u_i\}_1^r$ is set of roots of $f(x)$. $\{u_i\}_1^r \subseteq E$. $r \le \deg f = n$

suppose $g(x) = \prod_1^r (x-u_i)$ $\tau \in \mathrm{Aut}_k E$ permutate $\{u_i\}_1^r$

$\therefore \tau g(x) = g(x)$. $g(x) = \sum_0^r a_i x^i$. $\therefore \tau(a_i) = a_i$.

since E is Galois over k

$\Rightarrow a_i \in k$. $\forall 0 \le i \le r$.

$\therefore g(x) \in k(x)$. but $(g(x), f(x)) = g(x)$.

$\deg g \le \deg f$ $\therefore f = g$ by irreducible.

$\therefore f$ is product of poly- of degree 1.

Two maps

i) F is extension of k, there's one-to-one correspondense between close intermediate field and close subgrop. by $E \mapsto E'$

ii) $F \supseteq k$. E is stable intermediate field of F and k. then $\mathrm{Aut}_k F / \mathrm{Aut}_E F \cong \mathrm{Aut}_k E$. which is group of extensible k-iso- of $\bar{E}$ (to F)

② Fundamental Theorem of Galois Theorem.

F is finite dimensional Galois extension of k. Then there is an one-to-one corresponderce between set of intermediate fields and set of close subgroups of $\mathrm{Aut}_k F$, st

i) L, m are intermediate fields. then $[L:m] = [m':L']$

ii) $\bar{E}$ is Galois intermediate field $\Leftrightarrow E' \triangleleft \mathrm{Aut}_k F$.

And $G/E' \cong \mathrm{Aut}_k E \cong \mathrm{Aut}_k F / \mathrm{Aut}_E F$

③ Some conclusions:

1. $k(x)$ over k.

i) x is algebraic over $k(f/g)$, $f/g \notin k$.

ii) If $E \neq k$, an intermediate field, then

$[k(x) : E]$ is finite

iii) $x \longrightarrow f/g$ induce homo.: $\sigma : k(x) \to k(x)$, $\sigma(f/g) = f(f/g)/f(f/g)$, $\sigma \in \mathrm{Aut}\, k(x)$

$\Leftrightarrow \max \deg\{f(x), g(x)\} = 1$

iv) If k is infinite field $\Rightarrow k(x)$ is

Galois over k.

If k is finite field $\Rightarrow k(x)$ since

Galois over k.

v) If k is infinite, the only close groups

of $\mathrm{Aut}_k k(x)$ are itself and finite subgrp.

pf: i) Construct $\varphi(y) = \frac{f(x)}{g(x)} g(y) - f(y)$, s.t. $\varphi(x) = 0$

then we claim: $\varphi(y)$ is irreducible in $k(f/g)[y]$

By Gauss Lemma. $\Leftrightarrow$ in $k[f/g][y] = k[y][f/g]$

$\therefore f/g\, g(y) - f(y)$ has degree 1 is irred in $k[y][f/g]$.

$\therefore [k(x) : k(f/g)] = \text{degree } \varphi = \max\{\deg f, \deg g\}$.

(3) Some conclusions:

1. $k(x)$ over k.

i) x is algebraic over $k(f/g)$, $f/g \notin k$.

ii) If $E \neq k$, an intermediate field, then

$[k(x) : E]$ is finite

iii) $x \longmapsto f/g$ induce homo.: $\sigma : k(x) \to k(x)$ $\sigma(f/g) = f(f/g)/f(f/g)$, $\sigma \in \mathrm{Aut}\, k(x)$

$\Leftrightarrow \max \deg\{f(x), g(x)\} = 1$

iv) If k is infinite field $\Rightarrow k(x)$ is

Galois over k.

If k is finite field $\Rightarrow k(x)$ since

Galois over k.

v) If k is infinite, the only close groups

of $\mathrm{Aut}_k k(x)$ are itself and finite subgrp.

pf: i) Construct $\varphi(y) = \frac{f(x)}{g(x)} g(y) - f(y)$, s.t. $\varphi(x) = 0$

then we claim: $\varphi(y)$ is irreducible in $k(f/g)[y]$

By Gauss Lemma, $\Leftrightarrow$ in $k[f/g][y] = k(y)[f/g]$

$\therefore f/g\, g(y) - f(y)$ has degree 1 is irred in $k(y)[f/g]$.

$\therefore [k(x) : k(f/g)] = \text{degree } \varphi = \max\{\deg f, \deg g\}$.

2. $F \underbrace{\supseteq}_{\text{Galois}} E \underbrace{\supseteq}_{\text{Galois}} K$, $\forall \sigma \in \mathrm{Aut}_K E$. can be extended to

$\tilde{\sigma} \in \mathrm{Aut}_K F$. Actually. F is Galois over K. E is called stable.

3. Abouv Galois group:

F is finite Galois extension over K.

i) If L, M are intermediate field.

then $\begin{cases} \mathrm{Aut}_{L\cap M} F = \mathrm{Aut}_L F \cap \mathrm{Aut}_M F \\ \mathrm{Aut}_{L\cap M} F = \mathrm{Aut}_L F \vee \mathrm{Aut}_M F \end{cases}$

ii) If E is intermediate field. then

there's a unique smallest field L

s.t. $E \subseteq L \subseteq F$. L is Galois over K.

and $\mathrm{Aut}_L F = \bigcap_{\sigma \in \mathrm{Aut}_E F} \sigma (\mathrm{Aut}_E F) \sigma^{-1}$

Pf: i) 1) LM is close $\Leftrightarrow$ F is Galois over LM. $L\cap M$

For the former $\Longleftrightarrow$ $LM = (\mathrm{Aut}_L F \cap \mathrm{Aut}_M F)'$

$\{a \mid \sigma(a) = a, \sigma \in \mathrm{Aut}_L F \cap \mathrm{Aut}_M F\} = LM$

$= \{a \mid \sigma(a) = a, \sigma \in \mathrm{Aut}_M F\} \cap \{a \mid \sigma(a) = a, \sigma \in \mathrm{Aut}_L F\}$.

$= (\mathrm{Aut}_L F)' \cap (\mathrm{Aut}_M F)'$

2) $L\cap M = \{\sigma \mid \sigma(a) = a$. where $a \in L$ or $M\}$.

ii) 1) Note that $\mathrm{Aut}_E F$ is finite.

then find the maximal subgroup of $Aut_E F$.
which is $Aut_L F$. then we have L.

2) $\Leftarrow$ $L = \Pi(\sigma(Aut_E F)\sigma^{-1})'$

$= \Pi\{a \mid \sigma(Aut_E F)\sigma^{-1}(a) = a,\ \sigma \in Aut_K F\}$

$= \Pi\{a \mid (Aut_E F)\sigma^{-1}(a) = \sigma^{-1}(a),\ \sigma \in Aut_K F\}$

$= \Pi\{a \mid \sigma^{-1}(a) \in E,\ \sigma \in Aut_K F\}$

$= \Pi\, \sigma(E)$.

Since L is Galois over $K \Rightarrow L$ is stable

$\therefore\ \sigma(E) \subset L$. since $E \subseteq L$. $\therefore \Pi\sigma(E) \subseteq L$

On the other hand, $\cap \sigma(Aut_E F)\sigma^{-1} \trianglelefteq Aut_K F$

$\therefore \Pi(\sigma(Aut_E F)\sigma^{-1})'$ is stable and contain E.

(let $\sigma = id$) $\Rightarrow \therefore L \supseteq \Pi\sigma(E)$

(3) Splitting. Separable. Normal.

① Splitting:

Lemma. If $f \in k[x]$. $\deg f = n$. then exists a splitting field F of f over k. st. $[F:k] \leq n!$ and $[F:k] \mid n!$

Pf: By Induction on $\deg f$. choose a root from irreducible factor of f to make a simple intermediate extension!

3. Criteria.

i) for every extension field F of k, the maximal extension of k contains in F is k itself. then k is algebraic closure

ii) F is algebraically close. E consists all elements in F that are algebraic over k. then E is algebraic closure of k.

iii) F is algebraic closure of k $\Leftrightarrow$ $\forall$ extension E of k. $\exists$ k-mono: $E \to F$.

③ separable:

1. Some equivalent statements:

i) F is algebraic Galois extension of k

ii) F is separable over k and a splitting field of set of polynomials over k.

iii) F is splitting field of set of separable poly over k.

Def. Complete field: if $\forall f(x) \in F(x)$. $f(x)$ is irreducible, then $f(x)$ is separable.

$\Rightarrow$ Theorem: the algebraic extension of complete field is complete.

Pf: consider $\mathrm{char}\, F = p$. $\forall\, k \supseteq F$

Lemma. i) If $\mathrm{char}\, F = 0$, then F is complete field.
ii) If $\mathrm{char}\, F = p$, then F is complete field
$\Leftrightarrow F = F^p$

Pf: i) is trivial. For ii), If $f \in F[x]$ irred.
Then f is not separable $\Leftrightarrow f'(x) = 0$
$\Leftrightarrow f(x) = \sum_0^n a_i x^{ip}$, but $a_i = b_i^p$ by $F = F^p$
Then $f(x) = (\sum_0^n b_i x^i)^p$. contradiction!

$\Rightarrow$ It suffices to prove: $k^p = k$.

Homo: $\varphi: k \longrightarrow k$, $a \longmapsto a^p$ easy to see φ is homo

$\forall\, \alpha \in k$. Denote $E = F(\alpha)$
$[E : F] = [E/\ker\varphi : F/\ker\varphi]$
$= [\varphi(E) : \varphi(F)] = [\varphi(E) : F]$
$\because \varphi(E) \subseteq E \quad \therefore \varphi(E) = E$

$\forall f(x) \in k[x]$. Collect coefficients $\Rightarrow$ Simple extension.

Theorem: $\mathrm{char}\, F = p$. then $F(\alpha)$ is separable over F.
$\Leftrightarrow F(\alpha) = F(\alpha^p)$

Pf: ($\Rightarrow$) $\alpha \in F(\alpha^p) \Leftrightarrow \deg(\mathrm{irr}(\alpha, F(\alpha^p))) = 1$

~~Note that $\mathrm{irr}(\alpha, F(\alpha^p)) \mid \mathrm{irr}(\alpha, F)$~~

Construct: $x^p - \alpha^p \in F(\alpha^p)[x]$, which has a root α

But $irr(\alpha, F) \subseteq F[x] \subseteq F(\alpha^p)[x]$

Note $x^p - \alpha^p = (x-\alpha)^p$, $\therefore \alpha$ is the only root.

$\Rightarrow (irr(\alpha, F), x^p - \alpha^p) = x - \alpha$, by separability of $F(\alpha)$

$\therefore x - \alpha \in F(\alpha^p)[x]$ $\therefore \alpha \in F(\alpha^p)$

($\Leftarrow$) If $irr(\alpha, F)$ is not separable.

$\Rightarrow irr(\alpha, F) = \sum_0^n a_i x^{ip} = g(x^p) = \sum_0^n a_i x^i$

$\therefore g(\alpha^p) = 0 \Rightarrow [F(\alpha^p) : F] = \deg g$

$< \deg f = [F(\alpha) : F]$, contradiction!

Proposition: If $E = F(\alpha_1 \cdots \alpha_n)$ is separable over F.

then $\exists \theta$, s.t. $F(\theta) = E$.

Pf: Application: E is separable extension of k. k is separable over $F \Rightarrow E/F$ is separable!

Pf: $\Leftrightarrow$ $\forall \alpha \in E$, $irr(\alpha, F)$ is separable.

Note that $irr(\alpha, k) = \sum_0^n a_i x^i$ is separable.

Consider: $F \subseteq F([a_i]_0^n) \subseteq k$.

$\therefore irr(\alpha, k) = irr(\alpha, F([a_i]_0^n)) \in F([a_i]_0^n)[x]$.

($\Rightarrow$ prove: $F([a_i]_0^n)(\alpha)$ is separable over $F([a_i]_0^n)$

From $F(\{a_i\}_0^n) = F(\beta)$. We prove a Lemma.

Lemma. $F(\beta)/F$ separable extension. $\mathrm{char}\, F = p$

$F(\beta)(\alpha)/F(\beta)$ separable $\Rightarrow F(\beta)(\alpha)/F$ separable.

pf: $\Leftrightarrow$ α is separable over F. $\Leftrightarrow F(\alpha) = F(\alpha^p)$

Suppose $g(x) = \mathrm{irr}(\alpha, F(\alpha))$, $h(x) = \mathrm{irr}(\alpha, F(\alpha^p))$

$\because F(\alpha^p) \subseteq F(\alpha) \quad \therefore g(x) \mid h(x)$

Note that $(g(x))^p \in F(\alpha^p) \quad \therefore h(x) \mid g^p(x)$

But h, g are separable $\therefore h(x) = g(x)$

$[F(\alpha)(\beta) : F(\alpha)] = \deg g = \deg h = [F(\alpha^p)(\beta) : F(\alpha^p)]$

$= [F(\beta)(\alpha^p) : F(\alpha^p)] = [F(\beta)(\alpha) : F(\alpha^p)]$

$\Rightarrow$ We obtain $F(\alpha^p) = F(\alpha)$

Return to the proposition:

only prove: $F(\alpha, \beta)/F$ is separable $\Rightarrow F(\alpha, \beta) = F(\theta)$

(Actually the converse is true!)

then by Induction!

Consider Let $\theta = \alpha + c\beta$. test $F(\theta) \subseteq F(\alpha, \beta)$

Now prove $\exists c \in F$. s.t. $\beta \in F(\theta)$

$\Leftrightarrow x - \beta \in F(\theta)[x]$

suppose $f(x) = \mathrm{irr}(\alpha, F)$, $g(x) = \mathrm{irr}(\beta, F)$

$\Rightarrow f(x) = g(\beta) = 0 = f(\theta - c\beta)$, suppose $h(x) = f(\theta - cx)$

$\Rightarrow h(\beta) = 0$. We want $= (h(x), g(x)) = x - \beta$

Since $g(x)$ is separable, suppose $\{\beta_i\}_{i=2}^{n}$ $V[p]$ is set of roots of $g(x)$. we need to find "c" s.t. $h(\beta_i) \neq 0, \forall i$ $\Leftrightarrow$ Suppose $\{\alpha_j\}_j^m$ is set of roots of $f(x)$, $\theta - c\beta_i \neq \alpha_j$, $\because \theta = \alpha + c\beta$ $\therefore c(\beta - \beta_j) \neq \alpha_i - \alpha$.

$\therefore c \notin \left[\frac{\alpha_j - \alpha}{\beta - \beta_i} \mid 2 \leq i \leq n,\ 1 \leq j \leq m\right)$

If F is infinite field, it's true.

But if F is finite. then E is finite.

$\therefore E^* = \langle \beta \rangle$, β satisfies $x^{p^m} - x = 0$. It's simple extension.

④ Normal:

1. F is algebraic extension of k. the following statements are equivalent:

(i) F is normal over k.

(ii) F is splitting field over k of some set of polynomials in $k[x]$.

(iii) if $F \subseteq \bar{k}$. then for any k-mono. σ: $F \to \bar{k}$. $\sigma|_F \in Aut_k F$

Cor. F is Galois over $k \Leftrightarrow F$ is separable and normal!

Normal closure: E is algebraic extension of k.

extension F of E is normal closure

if: i) F is normal over k. which is the smallest containing E.

ii) If E/k is separable $\Rightarrow F/k$ is Galois.

and $[E:k]$ is finite iff $[F:k]$ is finite.

Moreover. F is unique determined up to E-iso

And **such normal closure always exists.**

Choose F is extension of $k(\alpha)$ over k.

$f(x)$ is irreducible poly of $k[x]$. the bases of E over k.

property

- i) $[F:k]=2 \Rightarrow F$ is normal over k.
- ii) If intermediate field E is normal over k. of $k \subseteq F$. $\Rightarrow E$ is stable. (converse is true when F/k is normal!)
- iii) each element of F belongs to a special intermediate field of $k \subseteq F$. $\Rightarrow$ F/k is normal!
- iv) F/k is normal $\Leftrightarrow$ every irreducible $f \in k[x]$. if factors in $F[x]$ as irreducible polys with the same degree.

(3) Generalize Galoss Theorem:

Replace "finite" by "Algebrase". For the the statements concerning index won't hold. Use separable to prove.

Theorem: 若 L, M are intermediate fields of $K \subseteq F$. L is finite dimensional Galoss extension of K. $\Rightarrow$ LM/M is finite and Galoss over M. With $Aut_M LM \cong Aut_{L\cap M} L$.

(4) Finite fields:

Property

i) F is finite field. char F = p. then $|F| = p^n$. $n = [F : Z_p]$.

ii) F is a field. $G < (F^*, *)$. $F^* = F/\{0\}$

$|G|$ is finite $\Rightarrow$ G is cyclic group

$\Rightarrow$ Cor. F is finite field. $(F^*, *)$ is cyclic group!

$\Rightarrow$ Cor. F is finite field, then F is simple extension of Z_p. denote $Z_p(m)$!

iii) $|F| = p^n$ ($\Leftarrow$) F is splitting field of $x^{p^n} - x$ over Z_p.

iv) Finite dimensional extension of finite field is Galois extension. And Galois group is cyclic!

(5) Some applications:

① Rule and Compass Construction

Fact: i) Rational numbers can be constructed.

ii) If c is constructible, then $\sqrt{c}$ can be constructed. If d can be constructed, then so $c \pm d$, cd, c/d

Note that the new points only generate from the intersections of lines, cycles, which means: every time $C_1 \cap C_2 \Rightarrow$ extend $\mathbb{Q} \to \mathbb{Q}(\sqrt{m})$. $\therefore$ every algebraic element is of degree 2^k over $\mathbb{Q}$, by compass & rule!

② Symmetric Rational functions:

Artin's Lemma: F is a field, $G < \mathrm{Aut}F$.

And $k = G' \Rightarrow F$ is Galois over k. Moreover, if $|G|$ is finite, then $[F:k]$ is finite.

$\Rightarrow$ Note that $S_n \longrightarrow \mathrm{Aut}_k k(x_1 \cdots x_n)$ is mono- ($\sigma(x_i) = x_{\sigma(i)}$. Def!), consider $S_n < \mathrm{Aut}_k k(x_1, \cdots x_n)$

Denote E is the set of symmetric polys $\in k(x_1 \cdots x_n)$

$\Rightarrow E = S_n'$, then $K(x_1 \cdots x_n)$ is finite (By $|S_n| = n!$) Galois extension over E with Galois group S_n.

$\Rightarrow$ Proposition: $|G|$ is finite, then exists a Galois field extension with Galois group $\cong G$.

Pf: By Cayley Theorem: $G \xrightarrow{\varphi} S_n$

then choose E_1 to be fix field of $\varphi(G)$

$\Rightarrow G \cong \mathrm{Aut}_{E_1} K(x_1 \cdots x_n)$

Consider $K(x_1 \cdots x_n)$ over E:

For $E_1 \subseteq E_1(x_1) \subseteq E_1(x_1, x_2) \cdots \subseteq E_1(x_1 \cdots x_n) = K(x_1 \cdots x_n)$, where $E_1 = K(f_1 \cdots f_n)$, $[f_i]_1^n$ is set of symmetric elementary

$\Rightarrow$ Note that $g_n(y) = \prod_1^n (y - x_i) \in K(f_1 \cdots f_n)[y]$

s.t. $g_n(x_n) = 0$. $\therefore [E_1(x_1 \cdots x_n) : E_1(x_1 \cdots x_n)] \le \deg g_n = n$.

$\Rightarrow [K(x_1 \cdots x_n) : E_1] \le n!$ $\therefore E_1 = E$.

And then $\{x_1^{s_1} \cdots x_n^{s_n} \mid 0 \le s_k < k\}$ is set of Basis of $K(x_1 \cdots x_n)$ over E.

③ Fundamental Theorem of Algebra

✡ $\mathbb{C}$ is algebraically closed.

Pf:

Lemma → if F is finite dimensional separable extension of infinite field $k \Rightarrow F = k(\alpha)$

→ $\forall$ such extensional field E doesn't exist:

$[E:\mathbb{C}]=2$. Since $\forall \deg g = 2$,

g splits in $\mathbb{C}$!

Pf: $\mathbb{C}$ has no proper extension except itself.

$\Rightarrow$ Consider Sylow-2-subgroup of $\mathrm{Aut}_{\mathbb{R}} E$.

Work odd order!

Relation of Galois. normal
. separable. stable :

· If F is extension of k. E is intermediate field