1. Isomorphism Theorem

① $\varphi: R_1 \to R_2$, $R_1/\ker\varphi \simeq \mathrm{Im}\varphi \leq R_2$

(i). $\ker\varphi \lhd R_1$

Let $a, b \in \ker\varphi$

$\varphi(a+b) = \varphi(a) + \varphi(b) = 0 + 0 = 0$ shows $a+b \in \ker\varphi$

$\forall\ r_1, r_2 \in R_1$

$\varphi(r_1 a) = \varphi(r_1)\varphi(a) = \varphi(r_1)\cdot 0 = 0$

$\varphi(a r_2) = \varphi(a)\varphi(r_2) = 0\,\varphi(r_2) = 0$

Hence, $\ker\varphi$ is a two-sided ideal of R_1

(ii). $\mathrm{Im}\varphi \leq R_2$

Let $a', b' \in \mathrm{Im}\varphi$ where $\varphi(a) = a' \in R_2$, $\varphi(b) = b' \in R_2$, $a, b \in R_1$

Then $a' + b' = \varphi(a) + \varphi(b) = \varphi(a+b) \in \mathrm{Im}\varphi$

and $a'b' = \varphi(a)\varphi(b) = \varphi(ab) \in \mathrm{Im}\varphi$

since $\mathrm{Im}\varphi \subseteq R_2$

Hence $\mathrm{Im}\varphi \leq R_2$

(iii) $R_1/\ker\varphi \simeq \mathrm{Im}\varphi$

Let $\psi: R_1/\ker\varphi \longrightarrow \mathrm{Im}\varphi$

$\quad r + \ker\varphi \longmapsto \varphi(r)$

①. well-defined Let $r_1, r_2 \in R_1$ s.t $r_1 - r_2 \in \ker\varphi$

Then $\varphi(r_1 - r_2) = 0 \Rightarrow \varphi(r_1) = \varphi(r_2)$

So $\psi(r_1 + \ker\varphi) = \varphi(r_1) = \varphi(r_2) = \psi(r_2 + \ker\varphi)$

So ψ is well-defined.

② homomorphism: let $r_1, r_2 \in R_1$

$\psi(r_1+\ker\varphi + r_2+\ker\varphi)$

$= \psi(r_1+r_2+\ker\varphi)$

$= \varphi(r_1+r_2)$

$= \varphi(r_1)+\varphi(r_2)$

$= \psi(r_1+\ker\varphi)+\psi(r_2+\ker\varphi)$

$\psi((r_1+\ker\varphi)(r_2+\ker\varphi))$

$= \psi(r_1r_2+\ker\varphi) = \varphi(r_1r_2) = \varphi(r_1)\varphi(r_2) = \psi(r_1+\ker\varphi)\psi(r_2+\ker\varphi)$

③ Surjective. it's obvious

④ Injective. if $\psi(r+\ker\varphi)=0 \Rightarrow \varphi(r)=0 \Rightarrow r\in\ker\varphi \Rightarrow r+\ker\varphi=\ker\varphi$

From ①②③④, ψ is an isomorphism, i.e. $R/\ker\varphi \simeq \operatorname{Im}\varphi$

② Consider $\pi: \begin{array}{l} R \to R/I \\ r \mapsto r+I \end{array}$

(1) $\left\{\begin{array}{l}\text{subring of } R \\ \text{containing } I\end{array}\right\} \xleftrightarrow{1:1} \{\text{subring of } R/I\}$

Let $I \lhd S \leq R$, $\pi(S)$ is a subring of R/I $(\operatorname{Im}\pi \leq R/I)$

Let $\bar{S} \leq R$ Consider the full preimage of $\bar{S}$. $\pi^{-1}(\bar{S})$

It's easy to check $\pi^{-1}(\bar{S}) \leq R$ and $I \lhd \pi^{-1}(\bar{S})$

Thus $\{\ \} \xleftrightarrow{1:1} \{\ \}$

$S \longrightarrow \pi(S)$

$\pi^{-1}(\bar{S}) \longleftarrow \bar{S}$

We establish a one-to-one correspondence.

(2) If $I \lhd J \lhd R$ then $J/I \lhd R/I$ and $R/J \simeq \dfrac{R/I}{J/I}$

Let $\varphi: R/I \longrightarrow R/J$

$r+I \longmapsto r+J$

It's easy to check this φ is a ring homomorphism.

Consider $\varphi(r+I) = J$ it shows $r \in J \Rightarrow \ker\varphi \subseteq J/I$, also $J/I \subseteq \ker\varphi$

Then $\ker\varphi = J/I$

Thus $R/I \big/ J/I \cong R/J$

③ $I \lhd R$, $S \leq R$, then $I+S \leq R$ and

(1). $S\cap I \lhd S$ and $I \lhd I+S$

$\forall$ $a, b \in S\cap I$. $s \in S$

$a+b \in S\cap I$, $sa \in S\cap I \Rightarrow S\cap I \lhd S$

Since $I+S$ is subring of R which containing I, $I \lhd I+S$

(2). $I+S/I \cong S/S\cap I$

Let $\varphi: S \longrightarrow S+I/I$

$s \longmapsto s+I$

Then φ is a ring homomorphism.

Consider $\varphi(s) = I \Rightarrow s \in I \Rightarrow s \in S\cap I \Rightarrow \ker\varphi \subseteq S\cap I$, also, $S\cap I \subseteq \ker\varphi$

$\Rightarrow \ker\varphi = S\cap I \Rightarrow I+S/I \cong S/S\cap I$

2. $F = \mathbb{F}_3$, $p(x) = x^2+1$

1° check $p(x)$ irre.

spc $p(x) = f(x)g(x)$ where $f.g$ are not unit

Then $\deg f = \deg g = 1$, it shows $p(x)$ has root over F

But $p(0) = 1$ $p(1) = 2$ $p(2) = 2$

$\Rightarrow p(x)$ has no root over F $\Rightarrow p(x)$ is irreducible over F.

2° find a basis.

1 and x.

3. $End(G)$ where $G = \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$

Consider $G = \langle a \rangle \oplus \langle b \rangle$ where $o(a) = o(b) = n$

$\forall \varphi \in End(G)$ $\varphi(a) = a_{11} \cdot a + a_{12} b$

$\varphi(b) = a_{21} a + a_{22} b$ where $a_{ij} \in \mathbb{Z}/n\mathbb{Z}$

$\Rightarrow End(G) \simeq M_2(\mathbb{Z}/n\mathbb{Z})$

is 2×2 matrix ring over the base ring $\mathbb{Z}/n\mathbb{Z}$.

4. R fin. unital ring, $ab=1$, prove $ba=1$.

Consider map $\varphi:$ $R \longrightarrow R$

$r \longmapsto br$

if $\exists r_1 \neq r_2$ s.t $br_1 = br_2$

then $r_1 = (ab)r_1 = a(br_1) = a(br_2) = (ab)r_2 = r_2$ ↯

Then φ is injective. Since $|R|<\infty \Rightarrow \varphi$ is also surjective

Thus φ is bijective, i.e $\exists\, s\in R$

s.t $\quad \varphi(s)=bs=1$

$\Rightarrow \quad a=a\cdot(bs)=(ab)s=s \quad \Rightarrow ba=1.$

5. if a nil, then $1-a$ invertible.

a nil $\Rightarrow \exists\, N\in\mathbb{N}$ s.t $a^N=0$

$\Rightarrow \quad 1=1-a^N=(1-a)(1+a+a^2+\cdots+a^{N-1}) \Rightarrow 1-a$ invertible.

6. $N=\{a\in R \mid a$ is nil element$\}$ is an ideal.

$\forall\, a,b\in N$, then a,b are nil elements

$\exists\, m,n\in\mathbb{N}$ s.t $\quad a^m=b^n=0$

Let $s\in\mathbb{N}$ s.t $\quad s=m+n+1$

Since R is commutative, $\quad (a+b)^s=\sum_{k=0}^{s} C_s^k a^k b^{s-k}=0$

Hence $\quad a+b\in N$

Furthermore, $\forall r\in R$, $\quad (ra)^m=r^m a^m=0$

$\Rightarrow N \trianglelefteq R$

7. prove distribution law of ideals in R with identity.

$\forall\, i,j,k\in I,J,K$ respectively.

$(i+j)k=ik+jk\in IK+JK \quad\Rightarrow\quad (I+J)K\subset IK+JK$

On the other hand

$\sum_{fin} i_s k_s + \sum_{fin} j_s k_s' \in IK + JK$ where $i_s \in I$, $j_s \in J$, $k_s, k_s' \in K$

Then $\sum_{fin} i_s k_s \in I$, $\sum_{fin} j_s k_s' \in J$

and $\sum_{fin} i_s k_s + \sum_{fin} j_s k_s'$

$= \sum_{fin} (i_s + 0) k_s + \sum_{fin} (0 + j_s) k_s' \in (I+J)K \Rightarrow IK + JK \subseteq (I+J)K$

Thus $(I+J)K = IK + JK$

Similarly, $K(I+J) = KI + KJ$

8. prove $M_n(K)$ is simple (K field)

Sps $0 \neq I \lhd M_n(K)$

Then $\exists$ $A \in I$ s.t $A = (a_{ij})$, and $\exists$ $1 \leq i, j \leq n$ s.t $a_{ij} \neq 0$

Since K field, a_{ij} is a unit

$\Rightarrow a_{ij}^{-1} A \in I \Rightarrow \hat{A} = a_{ij}^{-1} A = (b_{ij})$ and $b_{ij} = 1$

$\forall$ $1 \leq s, t \leq n$

$E_{si} \hat{A} E_{jt} = E_{st} \Rightarrow E_{st} \in I$

Since s, t are arbitrary, $M_n(K) = (E_{st})_{1 \leq s, t \leq n}$.

$\Rightarrow I = M_n(K)$

9. Let R be a non-zero commu. ring with identity. Prove

R simple ring $\Leftrightarrow$ R is a field.

$(\Rightarrow)$

As we all know, commutative division ring is field.

So only need to show $R\setminus\{0\} = U(R) = \{\text{unit of } R\}$

Suppose $\exists\, a \in R$. s.t $0 \neq a \notin U(R)$. i.e. a is not invertible

now (a) is a non-trivial ideal of R. contradict to

R is a simple ring

($\Leftarrow$) Since R is a field, R has no non-trivial ideal

$\Rightarrow R$ is simple ring.

10. $\varphi: K \to R$ homomorphism. $\varphi(K) = \{0\}$ or φ injective.

$\ker\varphi \trianglelefteq K$ shows $\ker\varphi = \{0\}$ or $\ker\varphi = K$

11. Prove: finite integral domain is field.

Let R be a finite integral domain

Consider map: $\varphi: R \to R$, $r \mapsto ar$ for some $a \neq 0, a \neq 1, a \in R$

Then φ is injective. Since $|R| < \infty$. φ also surjective

$\Rightarrow \varphi$ is bijective $\Rightarrow \exists\, b$ s.t $\varphi(b) = ab = 1$

$\Rightarrow a$ invertible $\Rightarrow R/\{0\}$ are invertible elements $\Rightarrow R$ is a field.

12. Prove all subgrup of Q_8 are normal.

Subgrup of Q_8 are $\{1\}$. Q_8 are

$\{\pm 1\}$ $\{\pm 1, \pm I\}$ $\{\pm 1, \pm j\}$ $\{\pm 1, \pm k\}$

They are all " union of conjugacy classes "

So they are are normal subgroup.

B. Hua's identity:

$$(a-aba)(a^{-1}+(b^{-1}-a)^{-1})$$

$$= 1-ab + a(b^{-1}-a)^{-1} - aba(b^{-1}-a)^{-1}$$

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

$$= 1-ab+ab = 1$$

14. Prove $(a+b)^p = a^p+b^p$, $\forall a, b \in F$. $\operatorname{char} F = p$

$$(a+b)^p = \sum_{k=0} C_p^k a^k b^{p-k} = a^p+b^p$$