Abstract Algebra

$Proposition:$

$(a\rangle = \bigcap\{I\ is\ left\ ideal\ of\ R\ containing\ a\} = \{na + ra | n \in Z,\ r \in R\}$

$Proof:$

$first\ prove\ (a\rangle\ is\ a\ left\ ideal\ containing\ a:$

$suppose\ a = 1_z \cdot a + 0_R \cdot a \in (a\rangle,\ n_1a + r_1a,\ n_2a + r_2a \in (a\rangle$

$(n_1a + r_1a) - (n_2a + r_2a) = (n_1 - n_2)a + (r_1 - r_2)a \in (a\rangle$

$\forall b \in R,\ b(na + ra) = nba + bra = 0_z \cdot a + (nb + br)a \in (a\rangle$

$then\ prove\ \forall a_0 \in (a\rangle,\ a_0 \in I:$

$suppose\ a_0 = na + ra \in I, a \in I \therefore ra \in I$

$$na = \begin{cases} a + a + ... + a & n > 0 \\ 0 & n = 0 \\ (-a) + (-a) + ... + (-a) & n < 0 \end{cases}$$

$\therefore na \in I \therefore a_0 = na + ra \in I,\ thus\ (a\rangle \subseteq I$

$Proposition:$

$(Z, +, \cdot)\ is\ PID(commutative\ principle\ ideal\ domain)$

$Proof:$

$I = \{0\} = (0) = Z \cdot 0 = \{0\},\ thus\ \{0\}\ is\ a\ principle\ ideal\ ring$

$I \neq \{0\},\ \exists n \in I(n \neq 0),\ (-n) = 0 - n \in\ I$

$without\ loss\ of\ generalization,\ let\ n \in I,\ n > 0\ and\ n\ is\ the\ least$

$then\ prove\ I = (n):$

$n \in I \therefore (n) \subseteq I$

$\forall m \in I,\ m = qn + r,\ 0 \leqslant r \leqslant n - 1 \Rightarrow r = m - qn$

$m \in\ I,\ qn \in (n) \subseteq I \therefore\ r \in I$

$by\ the\ choice\ of\ n\ as\ the\ least\ of\ positive\ elements\ in\ I,\ r = 0$

$\therefore m \in (n)\ \therefore\ I \subseteq (n) \therefore I = (n)$

$Proposition:$

$F[x]\ is\ a\ PID(suppose\ F\ is\ a\ field)$

$Proof:$

$0 \neq f(x) = a_n x^n + low...,\ a_n \neq 0$

$0 \neq g(x) = b_m x^m + low...,\ b_m \neq 0$

$f(x)g(x) = (a_n b_m)x^{n+m} + low...,\ a_n b_m \neq 0$

$\therefore F[x]\ is\ a\ domain.$

$Let\ I\ an\ ideal\ of\ F[x]$

$when\ I = \{0\},\ I = \{0\} = (0) = Z \cdot 0 = \{0\}$

$when\ I \neq \{0\},\ let\ f(x) \in I,\ f(x) \neq 0$

$suppose\ f(x)\ is\ a\ nonzero\ polynomial\ in\ I\ with\ the\ lowest\ degree$

$(f(x)) \subseteq I\ is\ obviously,\ then\ prove\ I \subseteq (f(x))$

$\forall g(x) \in I,\ g(x) = q(x)f(x) + r(x),\ r(x) = g(x) - q(x)f(x) \in\ I$

$thus\ r(x) = 0,\ thus\ g(x) = q(x)f(x) \subseteq (f(x)),\ thus\ I \in (f(x))$

$In\ addition,\ (f(x)) = \langle f(x)) = (f(x)\rangle = F[x] \cdot f(x)(commutative)$

$Proposition:$

$A\ matrix\ A\ is\ similar\ to\ a\ diagnal\ matrix\ if\ and\ only\ if$

$it\ has\ a\ splitting\ polynomial\ f(x)\ which\ has\ not\ multiplicity\ roots.$

$Proof:$

$A \sim (\lambda_1 E_1, ..., \lambda_r E_r) \Rightarrow P^{-1}AP = (\lambda_1 E_{n1}, ..., \lambda_r E_{nr}) := B$

$let\ f(x) = (x - \lambda_1) \cdot ... \cdot (x - \lambda_r)$

$\therefore 0 = f(B) = f(P^{-1}AP) = P^{-1}f(A)P \Rightarrow f(A) = 0$

$On\ the\ other\ side,\ f(x) = (x - \lambda_1) \cdot ... \cdot (x - \lambda_r),\ f(A) = 0$

$$let\ p_i(x) = \frac{f(x)}{x - \lambda_i} = (x - \lambda_1) \cdot ... \cdot (x - \lambda_{i-1})(x - \lambda_{i+1}) \cdot ... \cdot (x - \lambda_r)$$

$\therefore (p_1(x), ...p_r(x)) = 1,\ thus\ their\ greatest\ common\ factor\ is\ 1$

$\therefore\ there\ exist\ some\ g(x)\ such\ that$

$$F[x]p_1(x)+...+F[x]p_r(x)=(p_1(x))+...+(p_r(x))=F[x]g(x)$$
$$p_i(x)\in F[x]p_i(x)\subseteq F[x]g(x)\Rightarrow p_i(x)=q_i(x)g(x)\Rightarrow g(x)|p_i(x)$$
$$\therefore g(x)=1,\ 1\in F[x]\cdot 1=F[x]g(x)=F[x]p_1(x)+...+F[x]p_r(x)$$
$$\therefore \exists u(x)\in F[x]\ such\ that\ u_1(x)p_1(x)+...u_r(x)p_r(x)=1$$

$$Namely\ u_1(A)p_1(A)+...+u_r(A)p_r(A)=E$$
$$n=r(E)\leqslant r(u_1(A)p_1(A))+...+r(u_r(A)p_r(A)),\ if\ f(x)=0:$$
$$(x-\lambda_i)u_i(x)p_i(x)=u_i(x)f(x)=0\Rightarrow(A-\lambda_iE)u_i(A)p_i(A)=0$$
$$\therefore\ column\ vectors\ of\ u_i(A)p_i(A)\ is\ either\ 0\ or\ eigenvector\ related$$
$$to\ eigenvalue\ \lambda_i$$
$$\therefore\ r_i=r(u_i(A)p_i(A))\leqslant n_i(multicity\ of\ \lambda_i)$$
$$\therefore\ n\leqslant\ r_1+...+r_r\leqslant n_1+...+n_r=n\Rightarrow r_1+...+r_r=n$$

$Definition:$

$$homomorphism:\psi:R_1\to R_2\begin{cases}\psi(a+b)=\psi(a)+\psi(b)\\ \psi(ab)=\psi(a)\psi(b)\\ \psi(1)=1(with\ identity)\end{cases}$$
$$monomorphism: a\neq b\Rightarrow\psi(a)\neq\psi(b)$$
$$epimorphism:\forall r\in R_2,\exists a\in R_1\ s.t.\psi(r)=a$$
$$isomorphism=monomorphism+epimorphism+homomorphism$$

$Proposition:$

$The\ kernal\ of\ a\ homomorphism\ \psi:R_1\to R_2\ (ker\psi)\ is\ an\ ideal$

$Proof:$

$$\forall a,b\in ket\psi,\ \psi(a-b)=\psi(a)-\psi(b)=0-0=0\Rightarrow a-b\in ker\psi$$
$$\forall r\in R,\ \forall a\in ker\psi,\psi(ra)=\psi(r)\psi(a)=\psi(r)\cdot 0=0\Rightarrow ra\in ker\psi$$
$$notice: Im\psi=\{\psi(a)|a\in R_1\}\ is\ a\ subring\ of\ R_2\ but\ not\ an\ ideal$$
$$\psi:R_1\to R_2\ is\ injective\Leftrightarrow ker\psi=0$$

$Example:$

$$\psi:\mathrm{Z}\to\mathrm{Z}_n,\ a\to\bar{a}=\{a+kn|k\in\mathrm{Z}\}\ \psi(a+b)=\psi(a)+\psi(b),\ \psi(1)=\bar{1}$$
$$\psi(ab)=\psi(a)\psi(b),\ ker\psi=\{a\in\mathrm{Z}|\bar{a}=\bar{0}\}=n\mathrm{Z}=(n),\ Im\psi=\mathrm{Z}_n$$

$Definition:$

$Quotient\ ring: suppose\ I\ is\ an\ ideal\ of\ R,\ \frac{R}{I}=\{a+I|a\in R\}$

$(a+I)+(b+I)=(a+b)+I,\ (a+I)(b+I)=ab+I$

$Proposition:$

$a_1\neq a_2,\ a_1+I=a_2+I\Leftrightarrow a_1-a_2\in I$

$Proof:$

$\Rightarrow$

$a_1+I=a_2+I,\ 0\in I,\ a_1\in\{a_1+x|x\in I\}=a_1+I=a_2+I$

$\Rightarrow\exists x\in I\ s.t.a_1=a_2+x,\ x=a_1-a_2\in I$

$\Leftarrow$

$\forall a_1+x\in a_1+I\Rightarrow a_1+x=a_2+(a_1-a_2)+x\in a_2+I$

$a_1+I\subseteq a_2+I,\ a_1-a_2\in I\Rightarrow 0-(a_1-a_2)=a_2-a_1\in I$

$a+I=a'+I\Leftrightarrow a-a'\in I,\ b+I=b'+I\Leftrightarrow b-b'\in I$

$(a+b)+I\neq(a'+b')+I\Leftrightarrow(a+b)-(a'-b')=a-a'+b-b'\in I$

$\pi:R\to\frac{R}{I},\ r\to r+I$

$homomorphic\ and\ epimorphic\Rightarrow\ natural(cononical)$

$ker\pi=\{a\in R|a+I=0+I=I\}=I$

$Definition:$

$Maximal\ ideal: suppose\ I\ is\ an\ ideal\ of\ R,\ I\ is\ called\ to\ be\ maximal$

$if\ \forall J\lhd R,\ J\supseteq I\Rightarrow J=I\ or\ R(of\ course\ I\subseteq J\subseteq R)$

$Proposition:$

$suppose\ R\ is\ a\ commutatinve\ ring\ with\ identity\ 1_R$

$then\ M\ is\ a\ maximal\ ideal\Leftrightarrow\frac{R}{M}\ is\ a\ field$

$Proof:$

$\Rightarrow$

$\frac{R}{M} \neq \{0\},\ \forall r+M \in \frac{R}{M} \neq 0 \neq M \Leftrightarrow r-0 \notin M \Leftrightarrow r \notin M$

$(r)+M = Rr+M = (1\cdot r+0)+M \not\supseteq M \Rightarrow Rr+M = R$

$\therefore \forall x \in R, \exists a \in R, m \in M\ s.t.\ x = ra+m,\ substitude\ x = 1_R$

$\therefore 1 = ra+m,\ a \in R,\ m \in M$

$\therefore 1+M = ra+m+M = ra+M = (r+M)(a+M)$

$\Leftarrow$

$since\ \frac{R}{M}\ is\ a\ field,\ M \neq R,\ M \lhd R,\ M \not\subseteq J \lhd R(J\ is\ an\ ideal\ of\ R)$

$since\ M \neq J \therefore \exists r \notin M,\ r \in J,\ 0 \neq r+M \in \frac{R}{M}$

$suppose\ (r+M)(a+M) = ra+M = 1+M$

$\therefore \begin{cases} 1-ra \in M \subseteq J \\ ra \in J(r \in J) \end{cases} \Rightarrow 1 = (1-ra)+ra \in J$

$\therefore \forall x \in R,\ x = x\cdot 1 \in J \Rightarrow J = R$

$Definition:$

$suppose\ P \neq R\ is\ an\ ideal\ of\ R,\ R\ is\ commutitive\ with\ 1_R,\ then$

$P\ is\ called\ prime\ ideal,\ if\ \forall a,b \in R,\ ab \in P \Rightarrow either\ a \in P,\ or\ b \in P$

$Proposition:$

$P\ is\ a\ prime\ ideal\ of\ R(with\ 1_R) \Leftrightarrow \frac{R}{P}\ is\ a\ domain$

$Proof:$

$\Rightarrow$

$p \neq R,\ \frac{R}{P} \neq \{0\},\ a+P \neq 0,\ b+P \neq 0$

$\Rightarrow (a+P)(b+P) = ab+P \neq 0$

$(otherwise,\ ab \in P \Rightarrow a \in P\ or\ b \in P)$

$\Leftarrow$

$\frac{R}{P} \neq 0 \therefore P \neq R,\ \forall a,b \in R,\ ab \in P \Rightarrow ab+P = (a+P)(b+P)$

$also,\ ab+P = 0 \therefore a+P = 0\ or\ b+P = 0 \therefore a \in P\ or\ b \in P$

$Proposition:$

$suppose\ P\ is\ a\ prime\ ideal\ of\ R\ and\ R\ is\ a\ PID,\ then$

$P=0\ or\ P\ is\ maximal \Leftrightarrow P=pR=(p),\ ab\in P\Rightarrow a\in P\ or\ b\in P$

$(maximal\ ideal\rightarrow prime\ ideal,\ but\ the\ reverse\ is\ wrong)$

$Proof:$

$a\in P\therefore a\in(p)=RP\therefore a=rp\therefore p|a(of\ course\ p\neq 0\ and\ p\neq 1_R)$

$namely\ p|ab\Rightarrow p|a\ or\ p|b,\ such\ p\ is\ called\ prime\ element$

$a\ prime\ element\ in\ PID\ means\ its\ ideal\ is\ a\ prime\ ideal$

$Example:$

$not\ all\ rings'\ prime\ ideals\ are\ maximal\ ideals$

$suppose\ \psi:Z[x]\rightarrow Z,\ f(x)\rightarrow f(0)$

$ker\psi=\{f(x)|f(0)=0\}=xZ[x]=(x)$

$\dfrac{Z[x]}{ker\psi}=\{a+Z[x]x|a\in Z\}=\bar{a}+(x)$

$\psi:f(x)+ker\psi\rightarrow f(0)$

$\therefore\psi:Z[x]\rightarrow Z\ is\ isomorphic,\ \dfrac{Z[x]}{ker\psi}\ is\ a\ domain\ then\ Z\ is\ a\ domain$

$\therefore(x)\ is\ a\ prime\ ideal\ of\ Z[x]\ but\ x\ is\ not\ a\ maximal\ ideal$

$(because\ the\ quotient\ ring\ of\ a\ maximal\ must\ be\ a\ field)$

$Proposition$

$suppose\ R\ is\ a\ PID,\ P\ is\ a\ prime\ ideal\Leftrightarrow R_P\ =(p)\ is\ maximal$

$Proof:$

$suppose\ p\ is\ a\ prime,\ p\in R_P\subseteq R_a\subseteq R$

$p=ab\ for\ some\ b\Rightarrow p|ab\Rightarrow p|a\ or\ p|b$

$(1)p|a\Rightarrow a=pu=abu\Rightarrow a(1-bu)=0\Rightarrow bu=1$

$\quad pu=abu=a\in R_P\Rightarrow R_a=(a)\subseteq R_P\Rightarrow R_P=R_a$

$(2)p|b,\ b=pv,\ p=ab=apv=avp\Rightarrow av=1\in(a)=R_a$

$\quad\therefore\forall r\in R,\ r\cdot 1\in R_a\Rightarrow R=R_a$

$\Rightarrow R_P\ is\ a\ maximal\ ideal\ of\ R\ by\ (1)\ and\ (2)$

$$conversely,\ R_P\ is\ maximal,\ since\ R_P \neq R,\ p\ is\ not\ invertible,$$
$$p = 0 \Rightarrow \frac{R}{R_P} = \frac{R}{0} = R\ is\ a\ field$$
$$p \neq 0,\ p|ab \Rightarrow ab = pu \in (p) \Rightarrow R_P\ is\ maximal$$
$$\Rightarrow R_P\ is\ prime \Rightarrow \begin{cases} a \in (p) = R_P \Rightarrow a = r_1 p \Rightarrow p|a \\ b \in (p) = R_P \Rightarrow b = r_2 p \Rightarrow p|b \end{cases}$$

$Theorem:$
$R\ is\ PID,\ a \in R\ is\ irreducible \Leftrightarrow a\ is\ a\ prime$
$In\ general\ domain,\ all\ primes\ are\ irreducible\ but\ the\ reverse\ isn't.$
$in\ \mathbb{Z}[\sqrt{-5}],\ 2 \cdot 3 = (1 + \sqrt{5})(1 - \sqrt{-5}),\ 2\ is\ irreducible\ but\ not\ prime$

$Proof:$
$\Leftarrow$
$a\ is\ a\ prime \Rightarrow a = bc \Rightarrow a|bc \Rightarrow a|b\ or\ a|c$
$a|b,\ b = ar_1 \Rightarrow a = ar_1 c \Rightarrow r_1 c = 1,\ c\ is\ inveritible$
$a|c,\ c = ar_2 \Rightarrow a = br_2 a \Rightarrow br_2 = 1,\ b\ is\ inveritible$
$\Rightarrow a\ is\ irreducible$
$\Rightarrow$
$suppose\ p\ is\ irreducible,\ (p)\ is\ a\ maximal\ ideal\ of\ R,\ (p) \subseteq (a) \subseteq R$
$p \in (p) \subseteq (a) = R_a \Rightarrow p = ab\ for\ some\ b \in R,\ since\ p\ is\ irreducible$
$\Rightarrow a\ is\ invertible\ or\ b\ is\ invertible$
$a\ is\ invertible, \exists c\ s.t.\ ac = 1 \in (a) \Rightarrow (a) = R$
$b\ is\ invertible, \exists d\ s.t.\ bd = 1,\ p = ab \Rightarrow pd = a \in (p) \Rightarrow (a) = (p)$

$Proposition:$
$0 \neq f(x) \in Q[x], \exists c \in Q\ s.t.\ f(x) = cf_1(x),\ f_1(x) = a_n x^n + ... + a_0 \in Z[x]$
$f_1(x) = a_n x^n + ...a_0 \in Z[x]\ is\ said\ to\ be\ primitive,\ if\ the\ maximal$
$common\ divisor\ of\ a_0...a_n = 1\ or\ a_0...a_n\ are\ coprime$

$Gau\beta's\ lemma:$
$f(x)\ is\ irreducible\ in\ Q[x] \Leftrightarrow f_1(x)\ is\ irreducible\ in\ Z[x]$

$Proof:$

$\Rightarrow$

$suppose\ f_1(x)\ is\ not\ irreducible,\ then\ f_1(x) = g(x)h(x)$
$in\ which\ g(x) \neq \pm 1\ and\ h(x) \neq \pm 1,\ and\ g(x) \notin Z,\ otherwise$
$g(x)\ is\ a\ common\ divisor\ of\ (a_0 ... a_n),\ so\ does\ h(x)$
$\Rightarrow f(x) = (cg(x))h(x)\ is\ not\ irreducible,\ paradix\ to\ the\ suppose$

$\Leftarrow$

$suppose\ f_1(x)\ is\ irreducible,\ suppose\ f(x)\ = g(x)h(x)\ g(x), h(x) \notin Q$
$then\ \exists c_1, c_2 \in Q\ s.t. g(x) = c_1 g_1(x),\ h(x) = c_2 h_2(x),\ g_1(x)\ and\ h_1(x)$
$are\ primitive,\ c_1, c_2 \in Q \Rightarrow f(x) = cf_1(x) = c_1 c_2 g_1(x) h_1(x)$
$then\ if\ f_1(x) = \pm g_1(x) h_1(x),\ then\ f_1(x)\ is\ not\ irredubile,\ paradox$
$as\ for\ why\ f_1(x) = \pm g_1(x) h_1(x),\ we\ now\ give\ a\ proposition:$

$Proposition:$
$If\ g_1(x)\ and\ h_1(x)\ are\ primitive,\ then\ g_1(x) h_1(x)\ is\ primitive$

$Proof:$

$$consider\ g_1(x) = \sum_{i=0}^{n} a_i x^i,\ h_1(x) = \sum_{j=0}^{m} b_j x^j,\ g_1(x)h_1(x) = \sum_{k=0}^{m+n} c_k x^k$$

$in\ which\ c_k = a_0 b_k + ... + a_k b_0,\ conversely\ suppose\ p \mid g_1(x) h_1(x)$
$define\ w(x) = a_t x^t + ... + a_0,\ \bar{w}(x) = \bar{a}_t x^t + ... + \bar{a}_0,\ \bar{a}_i \in Z_p$
$given\ p\ is\ prime\ and\ Z\ is\ PID\ then\ Z_p[x] = \dfrac{Z}{p}\ is\ a\ field$
$\therefore \overline{g_1(x)h_1(x)} = \bar{0} = \overline{g_1(x)} \cdot \overline{h_1(x)} \Rightarrow \overline{g_1(x)} = \bar{0}\ or\ \overline{h_1(x)} = \bar{0},\ paradox$

$As\ proved\ above,\ g_1(x) h_1(x)\ is\ primitive,\ and\ f_1(x)\ is\ primitive$
$f_1(x) = (c^{-1}(c_1 c_2)) g_1(x) h_1(x) \Rightarrow (c^{-1}(c_1 c_2)) = \pm 1$

$Eisenstein's\ irreducible\ criterion:$
$f(x) = a_n x^n + ... + a_0 \in Z[x],\ p\ is\ a\ prime\ satisfying\ p \not| a_n,\ p \mid a_i$
$0 \leqslant a_i \leqslant n-1,\ p^2 \not| a_0,\ then\ f(x)\ is\ irreducible$

$Proof:$

$notice,\ the\ bar\ is\ unique\ for\ different\ p,\ where\ p\ can\ be\ an\ integer$
$on\ \mathbb{Z},\ a\ polynimial\ on\ \mathbb{Z}[x],\ or\ even\ a\ matrix\ on\ \mathbb{Z}[M]$
$conversely\ suppose\ f(x) = g(x)h(x) \Rightarrow \overline{f(x)} = \overline{g(x)} \cdot \overline{h(x)}$
$\Rightarrow \bar{a}_n x^n = \overline{g(x)} \cdot \overline{h(x)},\ on\ the\ other\ side,$
$g(x) = b_0 + ... + b_t x^t,\ h(x) = c_0 + ... + c_s x^s,\ \overline{g(x)} = \bar{b}_t x^t,\ \overline{h(x)} = \bar{c}_s x^s$
$\Rightarrow \bar{b}_0 = \bar{c}_0 = \bar{0} \Rightarrow p \mid b_0\ and\ p \mid c_0 \Rightarrow p^2 \mid b_0 c_0 = a_0,\ paradox\ to\ p^2 \not| a_0$

$An\ example\ of\ Eisenstein's\ irreducible\ criterion:$
$Show\ Q[\sqrt[n]{2}]\ is\ a\ number\ field.$
$Q[\sqrt[n]{2}] = \{a_0 + a_1\sqrt[n]{2} + ... + a_{n-1}\sqrt[n]{2^{n-1}} | a_i \in Q\},\ \psi: Q[x] \to Q[\sqrt[n]{2}]$
$f(x) \to f(\sqrt[n]{2}),\ then\ prove\ ker(\psi) = (x^n - 2)$
$f(x) \in ker(\psi),\ f(x) = (x^n - 2)g(x) + r(x),\ then\ 0 = f(\sqrt[n]{2}) = r(\sqrt[n]{2})$
$and\ the\ degree\ of\ r(x) \leqslant n$
$also,\ x^n - 2\ is\ irreducible(Eisenstein's\ criterion\ on\ situation\ p = 2)$
$r(x)\ and\ x^n - 2\ are\ not\ coprime(x - \sqrt[n]{2}\ is\ the\ only\ common\ root)$
$(r(x),\ x^n - 2) = x^n - 2,\ x^n - 2 \mid r(x) \Rightarrow r(x) = 0,\ ker(\psi) = (x^n - 2)$
$\therefore \dfrac{Q[x]}{ker(\psi)} \simeq Q[\sqrt[n]{2}] = \dfrac{Q[x]}{(x^n - 2)}\ is\ a\ field((x^n - 2)\ is\ a\ maximal\ ideal)$

$Proposition:$
$the\ ensemble\ of\ nilpotent\ in\ R(commutative)\ constitutes\ an\ ideal$

$Proof:$
$Denote\ I\ as\ the\ set\ of\ all\ nilpotent\ of\ R.\ First,\ if\ a\ is\ nilpotent,$
$then\ (-a)\ is\ also\ nilpotent,\ if\ a^m = 0,\ then\ a^m = a^{m+1} = ... = 0$
$\forall a, b \in I,\ their\ nilpotent\ exponents\ are\ k_1\ and\ k_2,\ then\ for$
$sufficiently\ large\ m >> k_1 + k_2,\ (a-b)^m = \sum_{i=0}^{m} \binom{n}{i} a^i (-b)^{m-i} = 0$
$\forall r \in R,\ (ra)^{k_1} = r^{k_1} a^{k_1} = 0,\ thus\ I\ is\ an\ ideal\ of\ R$

$Proposition:$
$(1)\ A\ ring\ whose\ nonzero\ elements\ are\ idempotents\ is\ commutative$
$(2)\ A\ ring\ with\ no\ zero\ elements\ and\ with\ some\ idempotents\ has$

$unique\ idempotent\ and\ is\ an\ unitary$

$Proof:$

$(1)\forall a\in R,\ a^2=a,\ (-a)^2=a^2=a=-a,\ \forall a\neq b\in R,\ a+b\neq 0$

$\therefore\ a+b=(a+b)(a+b)=a^2+b^2+ab+ba\Rightarrow ab=-ba=ba$

$(2)notice\ e(ea-a)=ea-ea=0\therefore ea=a,\ e\ is\ the\ unique\ unitary$

$Proposition:$

$Suppose\ \psi:R_1\to R_2\ is\ homomorphism,\ ker\psi=\{a\in R_1|\psi(a)=0\}$

$is\ an\ ideal\ of\ R,\ I\ is\ an\ ideal\ of\ R_1\ and\ I\subseteq\ker\psi,\ then\ there\ is\ a$

$homomorphism\ \bar{\psi}:\dfrac{R_1}{I}\to R_2\ s.t.\bar{\psi}(a+I)=\psi(a)$

$then\ it's\ easy\ to\ get\ ker\bar{\psi}=\{a+I|a\in ker\psi\}=\dfrac{ker\psi}{I},\ Im\bar{\psi}=Im\psi$

$Proof:$

$first\ prove\ \bar{\psi}\ is\ well-defined\ and\ homomorphism$

$a+I=b+I\Rightarrow a-b\in I\subseteq ker\psi,\ \psi(a-b)=0=\psi(a)-\psi(b)\Rightarrow$

$\psi(a)=\psi(b),\bar{\psi}(a+I)=\psi(a),\ \bar{\psi}(b+I)=\psi(b)\Rightarrow\bar{\psi}(a+I)=\bar{\psi}(b+I)$

$\bar{\psi}((a+I)(b+I))=\bar{\psi}(ab+I)=\psi(ab)=\psi(a)\psi(b)=\bar{\psi}(a+I)\bar{\psi}(b+I)$

$then\ prove\ \bar{\psi}\ is\ injective\ then\ bijective\ then\ isomorphism$

$ker\bar{\psi}=\{a+I\in\dfrac{R_1}{I}|\bar{\psi}(a+I)=0=\psi(a),\ a\in R_1\}=\{a+I|a\in ker\psi\}$

$Im\bar{\psi}=\{\bar{\psi}(a+I)|a\in R_1\}=\{\psi(a)|a\in R_1\}=Im\psi$

$\bar{\psi}\ is\ injective\Leftrightarrow ker\bar{\psi}=I\Leftrightarrow ker\bar{\psi}=\{0\}=\{a+I|a\in ker\psi\}$

$\forall a\in ker\psi,\ \bar{\psi}(a+I)=0,\ a+I\in ker\bar{\psi}=\{0+I\}$

$a+I=0+I\Rightarrow a=a-0\in I,\ ker\psi\subseteq I\Rightarrow I=ker\bar{\psi}$

$\Rightarrow\bar{\psi}:\dfrac{R_1}{ker\psi}\to Im\psi\ is\ isomorphism,\ bijiective,\ then\ homorphism$

$The\ first\ homomorphism\ fundemental\ theorem:$

$suppose\ \psi:R_1\to R_2\ is\ homo.,\ then\ \bar{\psi}:\dfrac{R_1}{ker\psi}\to Im\psi\ is\ isomorphism$

$The\ second\ homomorphism\ fundemental\ theorem:$

$suppose\ I,\ J\ are\ ideals\ of\ R\ and\ I \subseteq J,\ then:$

$(1): \dfrac{J}{I} = \{a + I | a \in J\}\ is\ an\ ideal\ of\ \dfrac{R}{I} \quad (2): \dfrac{R/I}{J/I} \simeq \dfrac{R}{J}$

$Proof:$

$\psi: \dfrac{R}{I} \to \dfrac{R}{J},\ \psi(a+I) = a + J,\ \psi\ is\ homomorphism\ is\ obviously$

$ker\psi = \{a + I \in \dfrac{R}{I} | \psi(a+I) = a + J = 0 + J\} = \{a + I \in \dfrac{R}{I} | a \in J\}$

$= \dfrac{J}{I}\ is\ an\ ideal\ if\ \dfrac{R}{I},\ then\ prove\ \psi\ is\ well-defined:$

$a + I = b + I \Rightarrow a - b \subseteq J \Rightarrow a + J = b + J \Rightarrow \psi(a+I) = \psi(b+I)$

$\therefore \dfrac{R/I}{J/I} = \dfrac{R/I}{ker\psi} \cong Im\psi = \dfrac{R}{J}$

$The\ third\ homomorphism\ fundemental\ theorem:$

$suppose\ S\ is\ a\ subring\ of\ R,\ I\ is\ an\ ideal\ of\ R,\ then:$

$(1): S + I\ is\ a\ subring\ of\ R\ \ (2): I\ is\ an\ ideal\ of\ S + I$

$(3): I \cap S\ is\ an\ ideal\ of\ S \quad (4): \dfrac{S+I}{I} \simeq \dfrac{S}{I \cap S}$

$Proof:$

$let\ s_1 + a_1, s_2 + a_2 \in S + I,\ s_i \in S,\ a_i \in I,\ then$

$(s_1 + a_1) - (s_2 + a_2) = (s_1 - s_2) + (a_1 - a_2) \in S + I$

$(s_1 + a_1)(s_2 + a_2) = s_1 s_2 + s_1 a_1 + s_2 a_2 + a_1 a_2 \in S + I$

$\psi: S \to \dfrac{S+I}{I}\ \psi(a) = a + I$

$\psi(ab) = ab + I = (a + I)(b + I) = \psi(a)\psi(b)$

$Im\psi = \{a + I | a \in S\} = \{s + a + I = s + I | s \in S,\ a \in I\} = \dfrac{S+I}{I}$

$ker\psi = \{a \in S | \psi(a) = a + I = 0 + I\} = I \cap S$

$\therefore \dfrac{S}{I \cap S} = \dfrac{S}{ker\psi} \simeq Im\psi = \dfrac{S+I}{I}$

$Example:$

$suppose\ F\ is\ a\ field,\ f(x) = a_0 + a_1 x + ... + a_{n-1} x^{n-1} + x^n,\ n \in N$

$\dfrac{F[x]}{(f(x))} = \{r_0 + r_1 x + ... + r_{n-1} x^{n-1} + (f(x)) | r_i \in F\}\ is\ a\ vector\ space$

$(f(x))$

$over\ F\ with\ basis\{\bar{1}, \bar{x},, ...\overline{x^{n-1}}\},\ \bar{1} = 1 + (f(x)),\ \bar{x} = x + (f(x))..$

$r_0 ... + r_{n-1}x^{n-1} + (f(x))\ is\ invertible \Leftrightarrow (r_0 + ... + r_{n-1}x^{n-1}, f(x)) = 1$

$Proof:$

$first\ prove\ \frac{F[x]}{(f(x))}\ is\ a\ vector\ space$

$\frac{F[x]}{(f(x))} = \{g(x) + (f(x)) | g(x) \in F[x]\},\ g(x) = q(x)f(x) + r(x)$

$g(x) - r(x) = q(x)f(x) = (f(x)) \therefore g(x) + (f(x)) = r(x) + (f(x))$

$r_0 + ... + r_{n-1}x^{n-1} + (f(x)) = (r_0 + (f(x))) + ... + (r_{n-1}x^{n-1} + (f(x)))$

$= r_0 + r_1(1 + (f(x))) + ... + r_{n-1}(x + (f(x)))^{n-1} = r_0\bar{1} + ... + r_{n-1}\overline{x^{n-1}}$

$notice: it's\ the\ first\ property\ of\ g(x)$

$suppose\ r_0\bar{1} + ... + r_{n-1}\overline{x^{n-1}} = r_0 + ... + r_{n-1}x^{n-1} + (f(x)) = 0 + (f(x))$

$then\ r_0 + r_1x + ... + r_{n-1}x^{n-1} - 0 \in (f(x)) = F[x]f(x)$

$r_0 + r_1x + ... + r_{n-1}x^{n-1} = (a_0 + a_1x + ... + x^n)g(x) = 0 \Rightarrow r_i \equiv 0$

$So\ these\ vectors\ are\ linearly\ independent$

$then\ prove\ the\ equivalence\ relation$

$\Rightarrow$

$(r_0 + r_1x + ... + r_{n-1}x^{n-1} + (f(x)))(g(x) + (f(x))) = 1 + (f(x))$

$Since\ this\ is\ a\ commutative\ ring,\ just\ prove\ one\ direction$

$\Leftrightarrow (r_0 + r_1x + ... + r_{n-1}x^{n-1})g(x) - 1 \in (f(x)) = f(x)h(x)$

$\Leftrightarrow (r_0 + r_1x + ... + r_{n-1}x^{n-1})g(x) - f(x)h(x) = 1$

$if\ p(x) \mid r_0 + r_1x + ... + r_{n-1}x^{n-1},\ p(x) \mid f(x),\ then\ p(x) \mid 1 \Rightarrow p(x) = 1$

$So\ the\ greatest\ common\ factor\ is\ 1(coprime)$

$\Leftarrow$

$conversely,\ (r_0 + r_1x + ... + r_{n-1}x^{n-1},\ f(x)) = 1$

$thus\ F[x](r_0 + r_1x + ... + r_{n-1}x^{n-1}) + F[x]f(x) = 1 = F[x]u(x)$

$for\ some\ u(x) \in F[x]:$

$u(x) = h_1(x)(r_0 + r_1x + ... + r_{n-1}x^{n-1}) + h_2(x)f(x)\ for\ some\ h_i(x)$

$since\ r_0 + r_1x + ... + r_{n-1}x^{n-1}, f(x) \in (F[x]u(x))$

$let\ r_0 + r_1x + ... + r_{n-1}x^{n-1} = v_1(x)u(x),\ f(x) = v_2(x)u(x)$

$\therefore\ u(x) \mid f(x),\ u(x) \mid r_0 + r_1x + ... + r_{n-1}x^{n-1} \Rightarrow u(x) = 1$

$Next,\ consider\ the\ method\ of\ inversion:$

$$1+(f(x))=h_1(x)(r_0+r_1x+...+r_{n-1}x^{n-1})+h_2(x)f(x)+(f(x))$$
$$=h_1(x)(r_0+r_1x+...+r_{n-1}x^{n-1})+(f(x))$$
$$=(h_1(x)+(f(x)))(r_0+r_1x+...+r_{n-1}x^{n-1}+(f(x)))$$

$Futhur\ more,\ \dfrac{F[x]}{(f(x))}\ is\ a\ field,\ namely$

$$r_0+r_1x+...+r_{n-1}x^{n-1}+(f(x))=0\Leftrightarrow r_0=r_1=...=r_{n-1}=0$$

$Proposition:$

$suppose\ p(x)\ is\ irreducible,\ f(x)=p(x)^nq(x)\ and\ p(x)\not|q(x),\ then$

$$\frac{F[x]}{(f(x))}\simeq\frac{F[x]}{(p(x)^n)}\oplus\frac{F[x]}{(g(x))}=\{(a+(p(x)^n),b+(g(x)))|a,b\in F[x]\}$$

$Proof:$

$$(\bar{a},\bar{b})+(\bar{c},\bar{d})=(\bar{a}+\bar{c},\bar{b}+\bar{d}),\ (\bar{a},\bar{b})(\bar{c},\bar{d})=(\bar{a}\cdot\bar{c},\bar{b}\cdot\bar{d})$$
$$\psi:\frac{F[x]}{(f(x))}\rightarrow\frac{F[x]}{(p(x)^n)}\oplus\frac{F[x]}{(g(x))},\ a+(f(x))\rightarrow(\bar{a},\bar{a})$$
$$(\bar{a},\bar{a})=(a+(p(x)^n),a+(g(x))),\ thus\ \psi\ is\ well-defined$$

$Also,\ \psi\ is\ a\ homomorphism:$

$$\psi((a+(f(x)))(b+(f(x))))=\psi(ab+(f(x)))=(\bar{a}\bar{b},\bar{a}\bar{b})=(\bar{a},\bar{a})(\bar{b},\bar{b})$$
$$ker\psi=\{a+(f(x))|(\bar{a},\bar{a})=0\}$$
$$a+(p(x)^n)=0\Rightarrow p(x)^n\mid a,\ a+(g(x))=0\Rightarrow g(x)\mid a$$
$$a=p(x)^nu(x)=g(x)\Rightarrow p(x)\mid g(x)v(x)\Rightarrow p(x)\mid g(x)\ ro\ p(x)\mid v(x)$$
$$\therefore p(x)\mid v(x),\ v(x)=v_1(x)p(x)$$

$Substitute\ into\ the\ equation\ representing\ a:$

$$p^n(x)u(x)=g(x)p(x)v_1(x),\ p^{n-1}(x)u(x)=g(x)p(x)v_2(x),...$$
$$\Rightarrow v(x)=p(x)^nv_n(x)\Rightarrow p(x)^nu(x)=g(x)p(x)^nv_n(x)=f(x)v_n(x)$$
$$\therefore f(x)\mid a\therefore ker\psi=\{0\}$$

$Also,\ \psi\ is\ surjective\ because\ dim\dfrac{F[x]}{(f(x))}=deg(f(x))$

$$dim(\frac{F[x]}{(p(x)^n)} \oplus \frac{F[x]}{(g(x))}) = dim(\frac{F[x]}{(p(x)^n)}) + dim(\frac{F[x]}{(g(x))})$$

ψ *is injective with same dimension on both sides* $\Rightarrow$ *surjective*

Therefore, let $f(x) = p_1(x)^{n_1} ... p_r(x)^{n_r}$, $p_i(x) \neq p_j(x)$, $i \neq j$ *then*

$$\frac{F[x]}{(f(x))} \cong \frac{F[x]}{(p_1(x)^{n_1})} \oplus ... \oplus \frac{F[x]}{(p_r(x)^{n_r})}$$

and Jordan matrix needs $p_i(x) = x - \lambda_i$ *to diagonalize*

Proposition :

Suppose p *is a prime,* $\mathbb{Z}_P = \{\bar{0}, \bar{1}, ..., \overline{p-1}\} = \frac{\mathbb{Z}}{p\mathbb{Z}}$ *is a field,* $|\mathbb{Z}_P| = p$

$\forall p$, F *is a field,* $n \in N^*$, *then* $\forall n, \exists F; \forall F, \exists N : |F| = p^n$

Example :

consider $x^3 + x + 1$ *is irreducible in* $\mathbb{Z}_2[x]$, *and we know the priciple ideal of prime element is a maximum ideal, and the quotient ring of the maximum ideal is a field, then a quotient ring* $\frac{\mathbb{Z}_2[x]}{(x^3+x+1)\mathbb{Z}_2[x]}$

$= \{a_0\bar{1} + a_1\bar{x} + a_2\bar{x}^2 | a_i \in \mathbb{Z}_2\}$; $\bar{1}, \bar{x}, \bar{x}^2$ *is a basis of* $\frac{\mathbb{Z}_2[x]}{(x^3+x+1)\mathbb{Z}_2[x]}$

$$\left|\frac{\mathbb{Z}_2[x]}{(x^3+x+1)\mathbb{Z}_2[x]}\right| = 8 = 2^3$$

Example :

Suppose $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$, $\frac{\mathbb{Z}[i]}{(p+i)} \cong \frac{\mathbb{Z}[x]/(X^2+1)}{(p+x, x^2+1)/(x^2+1)}$

$$\cong (2th.\ ring\ homo\ theorem) \frac{\mathbb{Z}[x]}{(p+x, x^2+1)} \cong \frac{\mathbb{Z}[x]/(x+p)}{(p+x, x^2+1)/(p+x)}$$

$$= \frac{\mathbb{Z}}{((-p)^2+1)} = \mathbb{Z}_{p^2+1}$$

$$\frac{\mathbb{Z}[x]}{(x+p)} = \{f(x) + (x+p) = g(x)(x+p) + r\} \Rightarrow r = f(-p), x = -p$$

Definition :

M *is an abelian group,* R *is a ring,* $R \times M \to M$, $(r, m) \to rm$ *has :*

$(r_1 r_2)m = r_1(r_2 m), (r_1 + r_2)m = r_1 m + r_2 m, r(m_1 + m_2) = rm_1 + rm_2$
$then\ M\ is\ a\ left\ R - module$

$Futhermore,\ if\ R\ has\ 1_R,\ and\ 1_R \cdot m = m, \forall m \in M,\ then\ M\ is\ a\ unitary$
$R\ is\ a\ division\ ring,\ R - module\ is\ also\ called\ vector\ space\ on\ R$

$Similarly,\ suppose\ M \times R \to M, m(r_1 r_2) = (mr_1)r_2,\ M\ is\ a\ left(right)$
$R - module,\ then\ M\ is\ a\ right(left)\ R^{op} - module,\ R^{op}\ is\ a\ ring,$
$(R^{op}, +) = (R, +),\ \forall a, b \in R^{op} = R,\ a \circ b := b \cdot a,\ (R^{op})^{op} = R$
$if\ R\ is\ a\ commutative\ ring,\ then\ R^{op} = R,\ also,$
$m \circ (r_1 \cdot r_2) = (r_1 \cdot r_2) \cdot m = r_1 \cdot (r_2 \cdot m) = (r_2 \cdot m) \circ r_1 = (m \circ r_2) \circ r_1$

$Example:$
$Suppose\ T\ is\ a\ linear\ endomorphism\ of\ F^n,\ R = F[x],\ R \times F^n \to F^n$
$(f(x), \alpha) \to f(t)(\alpha),\ then\ F^n\ is\ a\ F[x] - module$

$Hamidton - Caylay\ Theorem: A = (a_{ij})_{n \times n}, \exists f(\lambda) = |\lambda E - A|, f(A) = 0$
$T \to A: (Te_1, Te_2, ..., Te_n) = (e_1, e_2, ..., e_n)A,\ f(T)(\alpha) = 0(\alpha) = 0$
$but\ f(T) \neq 0\ and\ \alpha \neq 0,\ thus\ module\ is\ not\ a\ domain$

$Example:$
$\mathbb{Z}_m = \{\bar{0}, \bar{1}, ..., \overline{m-1}\},\ \mathbb{Z} \times \mathbb{Z}_m \to \mathbb{Z}_m,\ (k, \bar{r}) \to \overline{kr},\ \mathbb{Z}_m\ is\ \mathbb{Z} - module$
$but\ assume\ m \cdot \bar{r} = \overline{mr} = 0,\ m \in \mathbb{Z} \neq 0\ and\ \bar{r} \neq 0\ if\ m \not| r,\ thus$
$(\mathbb{Z}, +)\ is\ not\ a\ vector\ space\ over\ any\ field(so\ does\ F[x]^{F^n})$

$Definition:$
$\emptyset \neq N \subseteq R^M \Leftrightarrow \forall x, y \in N: x - y \in N; \forall r \in R, \forall x \in N: rx \in N,\ then$
$N\ is\ called\ a\ submodule\ of\ M$

$Property:$
$suppose\ N_1, N_2 \leqslant R^M,\ N_1 + N_2 \leqslant R^M,\ N_1 \cap N_2 \leqslant R^M,\ and\ N_1 + N_2$
$is\ a\ direct\ sum\ if\ N_1 \cap N_2 = \{0\},\ which\ is\ written\ as\ N_1 \oplus N_2$
$suppose\ N\ is\ a\ submodule\ of\ M,\ \dfrac{M}{N} = \{m + N | m \in M\}\ is\ a\ left$

$R-module,\ which\ is\ called\ quotient\ module\ of\ M\ by\ N$

$Example:$
$Suppose\ \{e_i|i\in J\}\ is\ a\ basis\ of\ N,\ N\ is\ a\ subspace\ of\ M\Rightarrow$
$\{e_i|i\in I,\ J\subseteq I\}\ is\ a\ basis\ of\ M,\ \{e_i+N|i\in\frac{I}{J}\}\ is\ a\ basis\ of\ \frac{M}{N}$
$also,\ if\ R\ is\ a\ field,\ then\ \frac{M}{N}\ is\ a\ vector\ space(quotient\ space)$
$the\ proof\ is\ similarly\ to\ linear\ space,\ thus\ obmitted$

$Property:$
$suppose\ \psi:R^M\rightarrow R^{M'}\ mapping,\ \psi(m_1+m_2)=\psi(m_1)+\psi(m_2),$
$\psi(rm)=r\ \psi(m),\ ker\psi=\{m\in M|\psi(m)=0\}\ is\ a\ submodule\ of\ R^M$
$Im\psi=\{\psi(m)|m\in M\}\ is\ a\ submodule\ of\ M',\ consider\ the\ first$
$fundamental\ theorem\ of\ ring\ homomorphism,\ \psi:M\rightarrow M'\ is\ homo$
$conseder\ M\rightarrow^{\psi}M'\Leftrightarrow M\rightarrow^{\pi}\frac{M}{ker\psi}\rightarrow^{\bar{\psi}}M',\ in\ which\ \pi(m)=m+ker\psi,$
$\bar{\psi}(m+ker\psi)=\psi(m)\Rightarrow\frac{M}{ker\psi}\simeq Im\psi=Im\bar{\psi}$

$Property:$
$N\leqslant L\leqslant M\Rightarrow\frac{M/N}{L/N}\cong\frac{M}{L};\ N,L\leqslant M\Rightarrow\frac{N+L}{L}\cong\frac{N}{N\cap L}$
$notice:if\ R\ is\ a\ field,\ it\ means\ two\ equivalent\ dimension\ formulas$

$Definition:$
$Suppose\ M\ is\ a\ left\ R-module,\ m_i\in M,\ r_i\in R,\ r_1m_1+...+r_nm_n\ is$
$a\ lenear\ combination\ of\ m_1,m_2,...,m_n\ then\ X=\{m_1,m_2,...,m_n\}$
$is\ the\ basis\ of\ the\ free\ module\ M,\ span(X)=\langle X\rangle=\bigcap_{N\supseteq\{m_1...m_k\}}N$
$=\{r_1m_1+...+r_km_k|r_i\in R\}$

$Proof:$
$\{r_1m_1+...+r_km_k|r_i\in R\}\ is\ a\ submodule\ containing\ m_1,m_2,...,m_k$
$(r_1m_1+..+r_km_k)-(r_1'm_1+..+r_k'm_k)=(r_1-r_1')m_1+..+(r_k-r_k')m_k$

$\therefore r(r_1m_1+...+r_km_k)=(rr_1)m_1+...+(rr_k)m_k \therefore span(X)\supseteq\langle X\rangle$
$also,\ N\leqslant M,\ r_1m_1+...+r_km_k\in N \therefore N\supseteq span(X) \therefore span(X)=\langle X\rangle$

$Thus\ span(X):=Rm_1+Rm_2+...+Rm_k,\ M\ is\ called\ a\ finitely$
$generated\ module\ if\ M=Rm_1+Rm_2+...+Rm_k$

$Example:$
$R=End_{\mathbb{R}}(\mathbb{R}[x])=\{\psi:\mathbb{R}[x]\to\mathbb{R}[x]\},\ \psi\ is\ well\ defined$
$(\psi(1),...,\psi(x^n),...)=(1,...,x^n,...)(a_{ij})_{\infty\times\infty}$
$R^R\ has\ basis\ 1_R=I_{\mathbb{R}[x]}$
$set\ f_1(x^{2n})=x^n,\ f_1(x^{2n+1})=0,\ f_2(x^{2n})=0,\ f_2(x^{2n+1})=x^n$
$consider\ a,b\in\{f_1,f_2\},\ af_1+bf_2=0,\ then\ prove\ a=0,\ b\ similarly$
$(af1+bf_2)(x^{2n})=af_1(x^{2n})=a(x^n)=0(x^{2n})=0\Rightarrow a=0$
$\forall f\in End_{\mathbb{R}}(\mathbb{R}[x]),\ f=af_1+bf_2,\ then\ f(x^{2n})=a(x^n),\ f(x^{2n+1})=b(x^n)$
$remark: it\ also\ shows\ that\ the\ basis\ of\ module\ is\ not\ necessarily\ unique$

$Proposition:$
$Suppose\ M\ is\ a\ finitely\ generated\ R-module,\ then\ there\ is\ an$
$epimorphism\ \psi:R^n\to M,\ satisfying\ M\cong\dfrac{R^n}{ker\psi}$

$Proof:$
$M\ is\ finitely\ generated,\ x_1...x_n\in M\ s.t.\ M=Rx_1+...+Rx_n$
$define\ \psi:R^n\to M\ (a_1,...,a_n)\to a_1x_1+...+a_nx_n,\ in\ which$
$\psi(\alpha+\beta)=\psi(\alpha)+\psi(\beta),\ \psi(r\alpha)=r\psi(\alpha),\ Im\psi=Rx_1+...+Rx_n=M$

$Example:$
$T\ is\ a\ linear\ transformation,\ F^n\to F^n(F\ is\ a\ field)$
$F^n\ is\ an\ F[x]-module,\ f(x)(\alpha)=f(T)(\alpha),\ \forall f(x)\in F[x],\ \forall\alpha\in F^n$
$F^n=F[x]e_1+...+F[x]e_n,\ \psi:F[x]^n\to F^n\ is\ epic\Rightarrow F^n\cong\dfrac{F[x]^n}{ker\psi}$

$Zorn's\ Lemma:$

$\Omega\ is\ a\ nonempty\ partial\ order\ set,\ \forall a_1 < ... < a_n < ... \exists a \in R\ s.t. a_i \leqslant a$
$then\ there\ is\ an\ element\ b \in \Omega\ satisfying\ \forall a \in \Omega,\ b \leqslant a \Rightarrow b = a$

$Definition:$
$Suppose\ R\ is\ a\ division\ ring,\ R^M\ has\ a\ basis,\ R^M\ is\ said\ to\ be\ simple$
$if\ M \neq 0,\ R^N \leqslant R^M \Rightarrow N = 0\ or\ N = M,\ R^M\ is\ said\ to\ be\ semisimple$
$if\ R^M = \sum_{i \in I} T_i,\ T_i\ are\ simple$

$Example:$
$R\ is\ a\ division\ ring,\ \forall R^M = \Sigma R_m\ is\ semisimple,\ \forall R_m\ is\ simple$
$0 \neq N \leqslant R_m = \{rm | r \in R\},\ rm \in N,\ rm \neq 0 \rightarrow r \neq 0,\ r^{-1}(rm) = m$
$thus\ Rm_{i_j}\ is\ a\ simple\ R-module,\ thus\ \{m_i | i \in I\}\ is\ linearly$
$independent\ and\ it\ is\ a\ basis\ of\ M$

$Lemma:$
$N\ is\ a\ submodule\ of\ a\ semisimple,\ M = \sum_{i \in I} S_i,\ where\ S_i\ is\ simple$
$then\ there\ is\ subset\ J\ of\ I\ satisfying\ M = N \oplus (\sum_{i \in J} \oplus S_i)$

$Proof:$
$when\ N = M,\ J = \emptyset,\ \sum_{i \in J} S_i = \{0\},\ when\ N \neq M,\ conversely\ suppose$
$\forall i_0 \in J,\ S_{i_0} \cap N \neq 0,\ S_{i_0} \leqslant S_{i_0} \Rightarrow S_{i_0} \cap N = S_{i_0} \Rightarrow S_{i_0} \subseteq N \Rightarrow M = N$
$\therefore\ \forall i_0 \in J,\ S_{i_0} \cap N = 0,\ \Omega = \{J \subseteq I | N \cap \sum_{i \in J} S_i = \{0\},\ \sum_{i \in J} = \sum_{i \in J} \oplus S_i\}$
$\Omega \neq 0 \therefore \exists maximal\ J = \{i_0\} \in \Omega \Rightarrow M = N \oplus (\sum_{i \in J} S_i) = N \oplus (\sum_{i \in J} \oplus S_i)$
$M \neq N + \sum_{i \in J} S_i,\ \exists j_0 \in I,\ S_{j_0} \cap (N + \sum_{i \in J} S_i) = 0,\ J' = J \cup \{j_0\}$
$J' \in \Omega,\ J' \not\supseteq J$
$R^M = \sum_{m \neq 0} Rm = \sum_{m \in B} \oplus R^M,\ B\ is\ a\ basis\ of\ R^M,\ m_1 ... m_k \in B,\ suppose$

$$0 = r_1 m_1 + ... + r_k m_k \in Rm_1 \oplus ... \oplus Rm_k \Rightarrow r_i m_i = 0,\ r_i \neq 0 \therefore m_i = 0$$

$Theorem:$
$Suppose\ D\ is\ a\ basis\ of\ M,\ {}_D D^M \simeq {}_D D^N \Leftrightarrow m = n,\ diag_D M = |B|$
$Lemma:$
$Suppose\ S_i,\ T_i\ are\ simple\ R-module\ S_1 \oplus S_2 \oplus ... \oplus S_n \simeq T_1 \oplus T_2 \oplus ... \oplus T_m$
$then\ n = m,\ S_i \simeq T_i\ \ up\ to\ order$

$Proof:$
$first\ prove\ n \leqslant m,\ similarly\ m \leqslant n \Rightarrow m = n$
$when\ n = 1,\ define\ \psi : S_1 \to T_1 \oplus ... \oplus T_m\ which\ is\ isomorphism,\ S_1\ is\ simple$
$\therefore T_1 \oplus ... \oplus T_m = \psi(S_1) \simeq S_1\ is\ simple \Rightarrow m = 1,\ n \leqslant m$
$when\ n > 1,\ \psi(S_1) \leqslant T_1 \oplus ... \oplus T_m,\ \exists \{i_1, ..., i_r\} \simeq \{1, ..., m\} s.t.$
$T_1 \oplus ... \oplus T_m = \psi(S_1) \oplus T_{i_1} \oplus ... \oplus T_{i_r},\ \psi : S_2 \oplus ... \oplus S_n \to T_{i_1} \oplus ... \oplus T_{i_r} \Rightarrow r = n$
$n - 1 \leqslant r \leqslant m - 1 \{i_1, ..., i_r\} \neq \{1, ..., m\},\ \psi(S_1) \oplus T_{i_1} \oplus ... \oplus T_{i_r} = T_1 \oplus ... \oplus T_m$
$\Rightarrow \psi(S_1) = 0 \Rightarrow n \leqslant m \Rightarrow m = n (use\ induction\ similarly)$