Abstract Albegra

CXC

Exercise .
Define F[x]$\times F_A^n \to F_A^n,\ (f(x),\alpha) \to f(A)\alpha,\ F_A^n$ is a module over F[x], and finitely generated by $\{e_1,...,e_n\}$, but as $\forall A_{n\times n}\exists$ f(x) s.t. f(A)=0, thus $f(x)e_i = f(A)e_i = 0,\ e_i$ is linearly dependent over F[x](so $\{e_i\}$ is not basis)

$\psi : F[x]^n \to F_A^n, (f_1(x),...,f_n(x)) \to f_1(A)e_1 + ... + f_n(A)e_n$ is an F[x]-module homomorphism, $Im\psi \supseteq \{\psi(a_1,...a_n)|a_i \in F\} = F^n \Rightarrow \psi$ is an epimorphism, then set$\{\alpha_i(x) = (-a_{1i},...,x-a_{ii},...,-a_{ni})\}$(column vectors of xE-A) $\psi(\alpha_i) = -a_{1i}e_1 - ... + (A - a_{ii}E)e_i - ... - a_{ni}e_n = (a_{1i},...,a_{ni}) - (a_{1i},...,a_{ni}) = 0,\ \therefore\ \alpha_i \in ker\psi,\ and\ ker\psi \supseteq F[x]\alpha_1 + ... + F[x]\alpha_n,\ \{\alpha_i\}$ is basis of $ker\psi$

Lemma .
Suppose R is a PID, then there is a maximal element in $\Omega = \{Ra|a \in B\} \neq \emptyset$

Proof.
Suppose $Ra_1 \subseteq ... \subseteq Ra_n \subseteq ...,\ Ra_i \in \Omega$, let $I = \bigcup_{i=1}^{\infty} Ra_i$, it's easy to prove that I is an ideal of R($\forall x, y \in I, \exists N s.t. x, y \in Ra_N,\ x - y \in Ra_N \subseteq I$). There is an element a s.t. I=Ra, $a \in Ra = \bigcup_{i=1}^{\infty} Ra_i$ $\therefore \exists m\ s.t.\ a \in Ra_m,\ \therefore I = Ra \subseteq Ra_m \subseteq I \Rightarrow I = Ra_m \in \Omega,\ \forall i, Ra_i \subseteq I = Ra_m,\ \forall i \geqslant m, Ra_i = Ra_m$. By Zorn's lemma, there is a maximal element in Ω □

Lemma .
Let $\{x_1,...,x_n\}$ be a basis of M over a PID R, and $x = a_1x_1 + ... + a_nx_n$ be a nonzero element of M. Then there is a basis $\{\xi_1,...,\xi_n\}$ of M, s.t. $\exists r \in R, \exists \xi_1 \in \{\xi_1,...,\xi_n\},\ a = r\xi_1,\ Rd = Ra_1 + ... + Ra_n;\ \forall i,\ d \mid a_i$

Proof.
Without loss of generality, we assume that $a_1a_2...a_m \neq 0\ and\ a_{m+1} = ... = a_n = 0$ by remembering x_i. When m=1, $a = r_1x_1,\ r = r_1,\ \{\xi_1,...,\xi_n\} = \{x_1,...,x_n\}$. When $m \geqslant 2$, assume inductively that the lemma holds for $m \leqslant k$, set m=k+1 and $\alpha := a_1x_1 + ... + a_kx_k$, then $L = Rx_1 + ... + Rx_k$ has a basis $\{\xi_1,...,\xi_k\}$ s.t. $\alpha = a\xi_1\ and\ Ra = Ra_1 + ... + Ra_k$, set $Rr = Ra + Ra_m,\ \exists u_1, u_m\ s.t.\ u_1a + u_ma_m = r$, since $a, a_m \in Rr,\ \exists s_1, s_m\ s.t.\ a = s_1r,\ a_m = s_mr,\ thus\ s_1u_1 + s_mu_m = 1$(R is PID), $\begin{pmatrix} u_1 & u_m \\ -s_m & s_1 \end{pmatrix}\begin{pmatrix} s_1 & -u_m \\ s_m & u_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow (\eta_1\ \eta_m) = (\xi_1\ x_m)\begin{pmatrix} s_1 & -u_m \\ s_m & u_1 \end{pmatrix} \Leftrightarrow (\xi_1\ x_m) = (\eta_1\ \eta_m)\begin{pmatrix} u_1 & u_m \\ -s_m & s_1 \end{pmatrix}$. So $\{\eta_1, \xi_2, ..., \xi_k, \eta_m, x_{m+1}, ..., x_n\}$ is a basis of M as $\{\xi_1, ...\xi_k, x_m, ..., x_n\}$ does. Moreover, $x = a_1x_1 + ... + a_mx_m = a\xi_1 + a_mx_m = s_1r\xi_1 + s_mrx_m = r\eta_1 \therefore \forall i,\ r \mid a_i$ □

Lemma .
d is a GCD of $(a_1, ..., a_m)$ if and only if $Ra_1 + ... + Ra_m = Rd$

Proof.
$\Rightarrow$
$d \mid a_i (1 \leqslant i \leqslant m) \Rightarrow a_i = b_id \in Rd \Rightarrow Ra_i \subseteq Rd \Rightarrow \Sigma Ra_i \subseteq Rd,\ set\ \Sigma Ra_i = Rr,\ a_i \in Rr \Rightarrow r \mid a_i \Rightarrow r \mid d,\ \because d \mid a_i,\ r = \Sigma x_ia_i,\ \therefore d \mid r \Rightarrow d = ur,\ r = vd,\ \therefore d = uvd \Rightarrow uv = 1,\ \Sigma Ra_i = Rr = Rvd = Rd$ we can find that two GCDs are in difference of an invertible element.
$\Leftarrow$
$a_i \in Ra_i \subseteq Rd \therefore a_i = rb_i \Rightarrow d \mid a_i,\ \forall c \mid a_i (1 \leqslant i \leqslant m),\ d = \Sigma x_ia_i \Rightarrow c \mid d,\ further,\ \forall x = a_1x_1 + ... + a_nx_n,\ \exists\{y_1, ..., y_n\}\ s.t. x = dy_1,\ d = gcd(a_1, ..., a_n)$ □

Theorem .
Let $N \leqslant M = Rx_1 + ... + Rx_n,\ \{x_1, ...x_n\}$ is a basis, R is PID, then there is a basis $\{y_1, ..., y_n\}$ *and* $r_i \in R(r_i \mid r_{i+1} \Leftrightarrow Rr_{i+1} \subseteq Rr_i)\ s.t.\{r_1y_1, ..., r_my_m\}$ *is a basis of* N

Proof.
When n=1, $M = Rx_1$, set $I = \{r \in R|rx_1 \in N\},\ 0 \cdot x_1 = 0 \in I \therefore I \neq \emptyset,\ and\ N \neq$, so it's easy to prove that I is an ideal, $\therefore I = Rr_1$(R is PID), then prove $N = Rr_1x_1$
first, $r_1x_1 \in N \Rightarrow Rr_1x_1 \subseteq N$, then, $\forall \alpha \in N \subseteq Rx_1 = M, \exists s \in R\ s.t. \alpha = sx_1 \in N \Rightarrow s \in I \Rightarrow s = u_1x_1, u_1 \in R \Rightarrow \alpha = sx_1 = u_1r_1x_1 \in Rr_1x_1 \therefore N \subseteq Rr_1x_1 \therefore N = Rr_1x_1$. Then prove r_1x_1 is basis of N:consider $dr_1x_1 = 0$, the $dr_1 = 0(\{x_1\}$ is a basis of M) and $I \neq \emptyset \Rightarrow r_1 \neq 0$, then d=0(R is PID), thus $\{r_1x_1\}$ is a basis of N.

When $n \geqslant 2$, set $\Omega = \{Rd|\exists x \in N, \exists basis\{\xi_1, ..., \xi_n\}\ of\ M\ s.t.\ x = d\xi_1 + ... + d_n\xi_n\}, 0 = x \in N\ then\ Rd = 0 \in \Omega$, by Zorn's lemma, there is a maximal element $Rr_1 \in \Omega \Rightarrow \exists\ basis\{y_1, ..., y_n\}, \exists a \in N\ s.t.\ d = r_1y_1 + ...r_ny_n,\ r_1y_1 \in N$ is obviously. Then prove $N = R_1y_1 \oplus (N \cap (Ry_2 + ... + Ry_n))$: let $r_1 = gcd(d, d_2, ..., d_n)$, then $\exists\{y_1, ..., y_n\}$ as basis of R_n s.t. $x = r_1y_1$, let $N' = N \cap (Ry_2 + ... + Ry_n),\ \therefore\ Rx \subseteq N,\ N' \subseteq N \Rightarrow Rx \subseteq N$. On the other side, $\forall y \in N \Rightarrow y = b_1y_1 + ... + b_ny_n \in Rx + N'$, then prove $r_1 \mid b_1$:$Rb_1 \in \Omega,\ Rr_1 + Rb_1 = Rd$ $\therefore u_1r_1 + v_1b_1 = d,\ v_1y + u_1x \in N$, only consider y_1, $v_1y + u_1x = (v_1b_1 + u_1r_1)y_1 + ... = dy_1 + ...\ \therefore Rd \in \Omega$ $\therefore Rb \subseteq Rr_1 \therefore r_1 \mid b_1 \therefore b_1 = a_1r_1,\ y = a_1r_1y_1 + ... + b_ny_n = a_1x + ... + b_ny_n \in Rx + N' \Rightarrow N = Rx \oplus N'$, then $N' = N \cap (Ry_2 + ... + Ry_n) \leqslant Ry_2 + ... + Ry_n$, by assumption of induction, $\exists\ basis\{z_2, ...z_n\} of\ Ry_2 + ... + Ry_n, \exists r_i \in R\ s.t.\{r_2z_2, ..., r_mz_m\}\ is\ basis\ of\ N' \Rightarrow \{y_1, z_2, ..., z_n\}\ is\ basis\ of\ Rx_1 + ... + Rx_n \Rightarrow$ $\{r_1y_1, r_2z_2, ...r_mz_m\}$ is basis of N and $r_i \mid r_{i+1}(2 \leqslant i \leqslant m - 1)$(by assumption of induction), then prove $r_1 \mid r_1 :$

Consider $\{y_1, z_2, ..., z_n\}$ is a basis of R^n, $\{r_1y_1, r_2z_2, ..., r_mz_m\}$ is a basis of N, notice that R is a PID, thus $Rr_1 + Rr_2 = Rd', 0 \neq r_1y_1 + _2y_2 = d'(uy_1 + vz_2) = d'\eta_1, \eta_1 \in \{\eta_1, ..., \eta_n\}$, $\{r_2z_2, ..., r_mz_m\}$, is a basis of N', thus $r_i \mid r_{i+1},\ Rr_1 \subseteq Rd' \in \Omega, \therefore Rr_1 = Rd'(maximal\ as\ Rr_1\ may\ as\ well\ defined) \therefore Rr_2 \subseteq Rr_1 \Rightarrow r_1 \mid r_2$ □

Theorem .
Suppose $A = (a_{ij})_{m \times n},\ a_{ij} \in R$(PID), $\exists$ invertivle matrices U,V s.t. $UAV = diag(d_1, ..., d_r, 0, ..., 0)$, in which $d_i \mid d_{i+1},\ \forall 1 \leqslant i \leqslant r - 1$

Proof. Define $\psi : R^n \to R^m,\ \alpha \to A\alpha$ is homomorphism, $Im\psi \leqslant R^m\ and\ ker\psi \leqslant R^n$, R^n is freemodule of R, thus $ker\psi$ is also free(by theorem above), $\therefore \exists basis\{y_1, ..., y_n\}\ of\ R^n,\ a_i \mid a_{i+1},\ a_i \in R$ s.t. these elements$\{a_{m+1}y_{m+1}, ..., a_ny_n\}$ is basis of $ker\psi$, then prove $\{y_{m+1}, ..., y_n\}$ is basis of $ker\psi :$
Consider $0 = \psi(a_iy_i) = a_i\psi(y_i),\ \psi(y_i) = (b_{i1}, ...b_{im}) \in R^m,\ \therefore\ a_i(b_{i1}, ..., b_{im}) = (a_ib_{i1}, ..., a_ib_{im}) = 0,\ and\ a_i \neq 0(because\ \{a_iy_i\}\ is\ basis),\ \therefore\ \ y_i \in ker\psi \therefore y_i = l_{m+1}a_{m+1}y_{m+1} + ... + l_na_ny_n,\ l_i \in R,\ \therefore$ $l_{m+1}a_{m+1}y_{m+1} + ... + (l_ia_i - 1)y_i + ... + l_na_ny_n = 0 \therefore l_ia_i = 1, a_i$ is invertible, $\therefore \{y_1, ..., y_m, a_{m+1}y_{m+1}, ..., a_ny_n\}$ is also basis, without loss of generality, set $a_i = 1,\ \psi((y_1, ..., y_n)) = \psi((e_1, ..., e_n)V) = (\psi(e_1), ..., \psi(e_n))V = (e'_1, ..., e'_m)AV,\ because\ (\psi(e_1), ..., \psi(e_n)) = (Ae_1, ..., Ae_n) = A = E_mA = (e'_1, ..., e'_m)A$, also, $\psi((y_1, ..., y_n)) = (\psi(y_1), ..., \psi(y_n)) = (\psi(y_1), ..., \psi(y_m), 0, ..., 0),\ Im\psi \leqslant R^m,\ \exists\{\beta_1, ..., \beta_m\}\ is\ a\ basis\ of\ R^m,\ \{\psi(y_1), ..., \psi(y_t)\}$ is a basis of $Im\psi,\ \exists b_1, ..., b_m\ s.t.\ \{b_1\beta_1, ..., b_t\beta_t\}\ is\ a\ basis\ of\ Im\psi,\ \forall 1 \leqslant i \leqslant t - 1,\ b_i \mid b_{i+1}$
notice:free module on communicative ring has unique rank.
$\psi(y_1, ..., y_n) = (e'_1, ..., e'_m)AV,\ \because \{\beta_1, ..., \beta_m\}\ is\ basis\ of\ R^m \therefore \exists P$ is invertible, $(\beta_1, ..., \beta_m) = (e'_1, ..., e'_m)P = (\beta_1, ..., \beta_m)PAV,\ \ since\ \{\psi(y_1), ..., \psi(y_t)\}\ and\ \{b_1\beta_1, ..., b_t\beta_t\}$ is a basis of $Im\psi,\ \therefore\ (\psi(y_1), ..., \psi(y_t))$ and $(b_1\beta_1, ..., b_t\beta_t) \cdot P',\ P'\ is\ invertible,\ \therefore (\beta_1, ...\beta_m)PAV = (\psi(y_1), .., \psi(y_n)) = (b_1\beta_1, .., b_t\beta_t, 0, .., 0)\left(\begin{smallmatrix} P' & 0 \\ 0 & E_{n-t} \end{smallmatrix}\right) = (\beta_1, .., \beta_t, \beta_{t+1}, .., \beta_m)diag(b_1, .., b_t, 0, .., 0)\left(\begin{smallmatrix} P' & 0 \\ 0 & E_{n-t} \end{smallmatrix}\right) \therefore PAV = diag(b_1, ..., b_t, 0, ..., 0)\left(\begin{smallmatrix} P' & 0 \\ 0 & E_{n-t} \end{smallmatrix}\right)$
$PAV\left(\begin{smallmatrix} P'^{-1} & 0 \\ 0 & E_{n-t} \end{smallmatrix}\right) = diag(b_1, ..., b_t, 0, ..., 0) \therefore set\ Q = V\left(\begin{smallmatrix} P'^{-1} & 0 \\ 0 & E_{n-t} \end{smallmatrix}\right),\ PAQ = diag(b_1, ..., b_t, 0, ..., 0)$ □

Exercise .
$E_{ij},\ E_{ij}(k),\ E_i(-1),\ E_{ij}^{-1} = E_{ij},\ E_{ij}(k)^{-1}(k),\ E_i(-1)^{-1} \in M(\mathbf{Z}_2)$ can be used below:
$\left(\begin{smallmatrix} 4 & -6 \\ 12 & 8 \end{smallmatrix}\right) \in M(\mathbf{Z}_2) \to \left(\begin{smallmatrix} 4 & 2 \\ 0 & 26 \end{smallmatrix}\right) \to \left(\begin{smallmatrix} 0 & 2 \\ -52 & 26 \end{smallmatrix}\right) \to \left(\begin{smallmatrix} 2 & 0 \\ 26 & -52 \end{smallmatrix}\right) \to \left(\begin{smallmatrix} 2 & 0 \\ 0 & -52 \end{smallmatrix}\right) \to \left(\begin{smallmatrix} 2 & 0 \\ 0 & 52 \end{smallmatrix}\right)$
$\left(\begin{smallmatrix} x-4 & 6 \\ -12 & x-8 \end{smallmatrix}\right)\ on\ Q[x] \to \left(\begin{smallmatrix} x-4 & 1 \\ -12 & \frac{1}{6}(x-8) \end{smallmatrix}\right) \to \left(\begin{smallmatrix} x-4 & 1 \\ -12-\frac{1}{6}(x-8)(x-4) & 0 \end{smallmatrix}\right) \to \left(\begin{smallmatrix} 1 & x-4 \\ 0 & -12-\frac{1}{6}(x^2-12x+32) \end{smallmatrix}\right) \to \left(\begin{smallmatrix} 1 & 0 \\ 0 & -\frac{1}{6}x^2+2x-\frac{52}{3} \end{smallmatrix}\right)$

Corollary .
$\forall x = a_1x_1 + ... + a_nx_n,\ \exists\{y_1, ..., y_n\},\ s.t. x = dy_1,\ d = gcd(a_1, ..., a_n)$, suppose $0 \neq (a_1, ..., a_n) \in \mathbf{Z}^n$ and $gcd(a_1, ..., a_n) = 1$, then $\exists\{y_1, ..., y_n\}$ as basis of Z^n s.t. $y_1 = gcd(a_1, ..., a_n)$ and $\exists$ invertible matrix $A = \left(\begin{smallmatrix} a_1 & ... & a_n \\ & A' & \end{smallmatrix}\right)$

Proof.
$0 \neq N \leqslant R^n$, then $\exists\{y_1, ..., y_n\}, \exists a_i \mid a_{i+1}\ s.t.\{a_1y_1, ..., a_my_m\}$ is a basis of N.When n=1, then conclusion is shown obviously, when n¿1, set $\Omega = \{Ra|\exists x \in N, \exists\{\alpha_1, ..., \alpha_n\}\ s.t.\ x = a\alpha_1 + ... + a_n\alpha_n\}$, by Zorn's lemma, $\exists\ maximal\ Rd \in \Omega \Leftrightarrow \exists 0 \neq x \in N, \exists\{\alpha_1, ..., \alpha_n\}\ s.t.\ x = d\alpha_1 + ... + d\alpha_n$ ☐

Corollary .
$N \leqslant R^n$, then $\frac{R^n}{N} \cong \frac{R}{(a_1)} \oplus ... \oplus \frac{R}{(a_m)} \oplus R^{n-m},\ a_i \mid a_{i+1},\ 1 \leqslant i \leqslant m - 1$

Proof.
$\exists\{y_1, ..., y_n\}$ as a basis of R, $\exists a_i \mid a_{i+1}\ s.t.\{a_1y_1, ..., a_my_m\}$ is basis of N, $\frac{R^n}{N} = \frac{R^n}{Ra_1y_1+...+Ra_my_m},\ \psi : R^n \to \frac{R^n}{N},\ (r_1, ..., r_n) \to r_1y_1 + ... + r_my_m + N$, then ψ is epimorphism, $(r_1, ..., r_n) \in ker\psi\ means\ r_1y_1 + ... + r_ny_n \in N,\ and\ N = Ra_1y_1 + ... + Ra_my_m,\ \therefore\ r_1y_1 + ... + r_ny_n = k_1a_1y_1 + ... + k_ma_my_m,\ \therefore r_i = k_ia_i,\ r_{m+1} = ... = r_n = 0 \therefore ker\psi = \{(k_1a_1, ..., k_ma_m, 0, ..., 0)|k_i \in R\},\ \therefore \frac{R^n}{N} \simeq \frac{R^n}{ker\psi} = \frac{R}{(a_1)} \oplus ... \oplus \frac{R}{(a_m)} \oplus R \oplus ... \oplus R = \frac{R}{(a_1)} \oplus ... \oplus \frac{R}{(a_m)} \oplus R^{n-m}$ ☐

Question .
Set $\alpha \neq \beta$ are two roots of $x^4 + 2x^3 + 6x^2 + 4x + 2$, prove $\mathbf{Q}[\alpha] \simeq \mathbf{Q}[\beta]$

Proof.
Considering Eisenstein's discriminant by p=2, $x^4 + 2x^3 + 6x^2 + 4x + 2$ is prime on $\mathbf{Q}[x]$, define $\psi : \mathbf{Q}[x] \to \mathbf{Q}[\alpha],\ g(x) \to g(\alpha),\ \psi$ is epimorphism, kerψ=$\{g(x) \mid g(\alpha) = 0\}$ $\forall h(x) \in ker\psi$, h(x)=g(x)f(x)+r(x), then $h(\alpha) = q(\alpha)f(\alpha) + r(\alpha),\ \therefore r(\alpha) = 0 \Rightarrow r(x) = 0$ notice (f(x),r(x)) are not coprime, $\therefore ker\psi \subseteq (f(x))$, and $(f(x)) \subseteq ker\psi$, thus $ker\psi = (f(x)) \therefore \mathbf{Q}[\alpha] \simeq \frac{\mathbf{Q}[x]}{(f(x))} \simeq \mathbf{Q}[\beta]$ ☐

Theorem .
R is a PID, $\forall 0 \neq a \in R,\ Ra \neq R$, then $\exists p_1, ..., p_r \in R$ are primes s.t. $a = p_1, ..., p_r$

Proof.
Conversely suppose $\Omega = \{Rr \neq R \mid r \neq p_1...p_{n_1}\ for\ some\ p_i\},\ \therefore Ra \in \Omega \neq \emptyset,\ \therefore \exists Rb \in \Omega\ is\ maximal,\ \therefore$ b is not prime, set $\Lambda = \{Rx|R \neq Rx \supseteq Rb\} \Rightarrow \exists maximal\ Rp_1,\ p_1 \mid b \Rightarrow b = p_1b_1 \Rightarrow Rb \subsetneq Rb_1 \neq R$(otherwise, if b is not invertible, then b=p_1 up to unit,then $Rb = Rbb_1^{-1} \notin \Omega$, paradox), $\therefore Rb_1 \notin \Omega,\ \therefore b_1 = p_2...p_s,\ \therefore b = p_1p_2...p_s$, paradox. So Ω must be empty. ☐

Theorem .
R is a PID, $\forall 0 \neq a \in R,\ Ra \neq R,\ a = p_1...p_r = q_1...q_s,\ p_i, q_j$ are primes, then r=s and $p_i = u_iq_j,\ Ru_i = R$, namely $a = \prod_i^n p_i = \prod_j^n q_j$ is unique up to order and unit.

Proof.
when r-1, $p_1 \mid q_1...q_s \Rightarrow p_1 \mid q_1(some\ q_1) \Rightarrow q_1 = up_1, a = p_1 = q_1...q_s \Rightarrow q_1 \mid p_1 \therefore p_1 = vq_1 = uvp_1 \therefore uv = 1 \therefore a = p_1vq_2...q_s = p_1 \therefore vq_2...q_s = 1 \therefore q_j$ is invertible(paradox); when $r \geqslant 2,\ p_1...p_r = up_1q_2...q_s \therefore p_2...p_r = (uq_2)q_3...q_s$, because the invertible element multiplied by prime element is still prime element, thus by the induction hypothesis, $r = s, p_i = q_j$ up to order and unit. ☐

Theorem .
Suppose R has identity, A_i are ideals of R satisfying $A_i + A_j = R, \forall i \neq j \Rightarrow \varphi : \frac{R}{A_1\cap...\cap A_s} \to \frac{R}{A_1} \oplus ... \oplus \frac{R}{A_s},\ a + (A_1 \cap ... \cap A_s) \to (a + A_1, ..., a + A_s)$ is a ring isomorphism, and $A_1 \cap ... \cap A_s = A_1...A_s$

Proof.
define $\psi : R \to \frac{R}{A_1} \oplus ... \oplus \frac{R}{A_s},\ a + (A_1 \cap ... \cap A_s) \to (a + A_1, ..., a + A_s)$, then obviously, ψ is a ring homomorphism and ker$\psi = A_1 \cap ... \cap A_s$, thus $\bar{\psi} : \frac{R}{ker\psi} \simeq Im\psi$ is ring homomorphism.Then prove ψ is surjective.

Thus we first prove $A_1+A_2=R \Rightarrow A_1+(A_2\cap A_3)=R \Rightarrow ... \Rightarrow A_1+(A_2\cap ...\cap A_s)=R \Rightarrow A_i+(A_1\cap ...\cap \hat{A}_i\cap ..\cap A_s)=R$(supposing proved)
then namely, we need to prove $\forall(a_1+A_1,...,a_s+A_s)\in Im\psi, \exists a\in R,\ s.t.\ (a_1+A_1,...,a_s+A_s)=\psi(a)=(a+A_1,...,a+A_s)$, in which $(a_1+A_1,...,a_s+A_s)=\sum\limits_{i=1}^{s}(0,...,a_i+A_i,...,0):=\sum\limits_{i=1}^{s}\psi(b_i)=\psi(\sum\limits_{i=1}^{s}b_i)$. Consider the above lemma is proved, then $\forall a_i\in R=A_i+(A_1\cap...\cap\hat{A}_i\cap..\cap A_s),\ a_i=b_i(\in A_i)+c_i(\in A_1\cap...\cap\hat{A}_i\cap..\cap A_s)$, then $a_i+A_i=(b_i+c_i)+A_i=c_i+A_i$, thus $\psi(a_i)=\psi(c_i)=(c_i+A_1,...,c_i+A_s)=(0,...,c_i+A_i,...,0)=(0,...,a_i+A_i,...,0)$, so we can set $\psi(\sum\limits_{i=1}^{s}b_i)=\psi(a)$, then the proposition is proved.
As for the lemma, R has 1_R, thus $R=R^2=(A_1+A_2)(A_1+A_3)=A_1(A_1+A_2+A_3)+A_2A_3$, and A_i are ideals, so $A_1(A_1+A_2+A_3)\subseteq A_1$ and $A_2A_3\subseteq A_2\cap A_3$, so the original $\subseteq A_1+(A_2\cap A_3)\subseteq R,\ \therefore A_1+(A_2\cap A_3)=R$. Similarly suppose $A_1+(A_2\cap...\cap A_k)=R$, then $R=R^2=(A_1+A_{k+1})(A_1+(A_2\cap...\cap A_k))\subseteq A_1+(A_2\cap ...\cap A_k)\cap A_{k+1}\subseteq R,\ \therefore A_1+(A_2\cap...\cap A_{k+1})=R$
Finally, $A_1A_2\subseteq A_1\cap A_2=(A_1\cap A_2)(A_1+A_2)=(A_1\cap A_2)A_1+(A_1\cap A_2)A_2\subseteq A_2A_1+A_1A_2=A_1A_2,\ \therefore A_1A_2=A_1\cap A_2$. Similarly, suppose $A_1...A_k=A_1\cap...\cap A_k$, then $(A_1...A_k)A_{k+1}=(A_1\cap...\cap A_k)A_{k+1}\subseteq ((A_1\cap...\cap A_k)\cap A_{k+1})(A_{k+1}+A_1\cap...\cap A_k)\subseteq A_1\cap...\cap A_{k+1},\ \therefore A_1\cap...\cap A_{k+1}=R$ ☐

Theorem .
p,q are prime in a PID R, and $Rp\neq Rq$, namely $\nexists$ unit s.t. p=uq, $\forall a\in R,\ a=up_1^{r_1}...p_s^{r_s},\ Rp_i\neq Rp_j, \forall i\neq j$, then $\frac{R}{Ra}\simeq\frac{R}{(p_1^{r_1})}\oplus...\oplus\frac{R}{(p_s^{r_s})}$

Proof.
Namely prove $Ra=Rup_1^{r_1}...p_s^{r_s}=(Rp_1^{r_1})...(Rp_s^{r_s})=\bigcap\limits_{i=1}^{s}(Rp_i^{r_i})$, to satisfy the conditions of the Chinese remainder theorem, namely prove $Rp_i^{r_i}+Rp_j^{r_j}=R, \forall i\neq j$.
$\forall$ I as ideal of R, define $\sqrt{I}=\{a\in R|a^n\in Rforsomen\}$, it's obviously that $\sqrt{I}$ is an ideal. Then consider $\sqrt{Rp_i^{r_i}+Rp_j^{r_j}},\ p_i,p_j\in\sqrt{Rp_i^{r_i}+Rp_j^{r_j}}$, thus $Rp_i+Rp_j\subseteq\sqrt{Rp_i^{r_i}+Rp_j^{r_j}}$, and R is PID so Rp_i and Rp_j are maximal, with $Rp_i\neq Rp_j$, thus $Rp_i+Rp_j\neq Rp_i$, thus $Rp_i+Rp_j=R$ and $1_R\in\sqrt{Rp_i^{r_i}+Rp_j^{r_j}}$, namely $\exists n$ s.t. $1^n=1\in Rp_i^{r_i}+Rp_j^{r_j},\ \therefore Rp_i^{r_i}+Rp_j^{r_j}=R$ ☐

Conclusion . M is finitely generated on PID R, then $M\cong\frac{R}{Rr_1}\oplus...\oplus\frac{R}{R_s}\oplus R^t=\frac{R}{Rp_1^{n_1}}\oplus...\oplus\frac{R}{Rp_k^{n_k}}\oplus R^t$

Lemma .
R is a PID, $\forall p\in R$ is prime, $\forall n\geqslant 1,\ \frac{R}{Rp^n}=\frac{R}{(p^n)}\neq$ some $A\oplus B,\ A,B\neq\emptyset$

Proof.
$\forall\emptyset\neq N\leqslant\frac{R}{(p^n)}$, $\because$ R is PID, and with homomorphism fundamental theorem, $R\geqslant Ra$, and $\frac{M}{N}\geqslant\frac{L}{N}$, in which $L\subseteq M$, thus $N=\frac{Ra}{(p^n)}$. Set $a=a_1p^r,\ p\not|a_1$, then $Ra_1+Rp^n=R$, thus $1_R=ua_1+vp^n$ for some $u,v\in R,\ p^r+(p^n)=(ua_1+vp^n)p^r+(p^n)=ua_1p^r+(p^n)=u(a+(p^n))\in R(a+(p^n))$, thus $R(p^r+(p^n))\subseteq R(a+(p^r))\subseteq R(p^r+(p^n)),\ \therefore R(a+(p^r))=R(p^r+(p^n))$. Conversely suppose $\frac{R}{(p^n)}=A\oplus B=R(p^r+(p^n))+R(p^s+(p^n))$, then $R(p^r+(p^n))\cap R(p^s+(p^n))=R(p^{max\{s,r\}}+(p^n))$, and $R(p^r+(p^n))\neq 0\Leftrightarrow r<n$, thus Their intersection cannot be $\emptyset$. ☐

Theorem .
Suppose $M=\frac{R}{(p_1^{r_1})}\oplus...\oplus\frac{R}{(p_k^{r_k})}=\frac{R}{(q_1^{s_1})}\oplus...\oplus\frac{R}{(q_l^{s_l})}$, then k=l, and $Rp_i^{r_i}=Rq_i^{s_i}$ up to order, and $r_i=s_i$, $p_i=q_i$ up to unit.

Proof.
Let $\lambda_i:\frac{R}{(p_i^{r_i})}\to M,\ x\to(0,...,x,...,0)$, x is the i_{th} entry, $\lambda_i':\frac{R}{(q_i^{s_i})}\to M,\ x\to(0,...,x,...,0)$; and $\pi_i:M\to\frac{R}{(p_i^{r_i})},\ (x_1,...,x_i,...,x_k)\to x_i,\ \pi_i':M\to\frac{R}{(q_i^{s_i})},\ (x_1,...,x_i,...,x_l)\to x_i$. Thus $\sum\limits_{i=1}^{k}\lambda_i\pi_i=id_M=\sum\limits_{i=1}^{l}\lambda_i'\pi_i',\ \pi_1\lambda_1=1_{\frac{R}{(p_1^{r_1})}}=\sum\limits_{i=1}^{l}\pi_1\lambda_i'\pi_i'\lambda_1:=\sum\limits_{i=1}^{l}\theta_i,\ \therefore\exists i_0$ s.t. θ_{i_0} is an isomorphism(unproved), may as well let

$\theta_1 = \pi_1\lambda_1'\pi_1'\lambda_1$ is isomorphism. Then $\pi_1'\lambda_1 : \frac{R}{(p_1^{r_1})} \to \frac{R}{(q_1^{s_1})}$ is homomorphism, then prove it's isomorphism. $\pi_1\lambda_1'(1-\pi_1'\lambda_1\theta_1^{-1}\pi_1\lambda_1') = (\pi_1\lambda_1' - \pi_1\lambda_1'\pi_1'\lambda_1\theta_1^{-1}\pi_1\lambda_1') = \pi_1\lambda_1' - \pi_1\lambda_1' = 0$, then prove $\frac{R}{q_1^{s_1}} = Im\pi_1'\lambda_1 \oplus ker(1-\pi_1'\lambda_1\theta_1^{-1}\pi_1\lambda_1')$, $\forall x \in \frac{R}{(q_1^{s_1})}$, $x = \pi_1'\lambda_1\theta_1^{-1}\pi_1\lambda_1'(x) + (x - \pi_1'\lambda_1\theta_1^{-1}\pi_1\lambda_1'(x))$, $\forall y \in ker\pi_1\lambda_1' = \pi_1'\lambda_1(x)$, $0 = \pi_1\lambda_1'(y) = \pi_1\lambda_1'\pi_1'\lambda_1(x) = \theta_1(x)$, θ_1 is isomorphism, $\therefore x = 0, y = \pi_1'\lambda_1(x) = 0$. Since $\frac{R}{(q_1^{m_1})}$ is indecomposable, $Im\pi_1\lambda_1' = \emptyset$ or $ker\pi_1\lambda_1' = \emptyset$, if $Im\pi_1\lambda_1' = \emptyset$, then $\pi_1\lambda_1' = 0 \Rightarrow \pi_1\lambda_1'\pi_1'\lambda_1 = \theta_1 = 0$, contradiction, $\therefore ker\pi_1\lambda_1' = \emptyset \Rightarrow \frac{R}{q_1^{s_1}} = Im\pi_1'\lambda_1$, so there is $\frac{R}{(p_1^{n_1})} \xrightarrow{\lambda_1} \frac{R}{(p_1^{n_1})} \oplus ... \oplus \frac{R}{(p_s^{n_s})} = \frac{R}{(q_1^{m_1})} \oplus ... \oplus \frac{R}{q_r^{m_r}} \xrightarrow{\pi_1'} \frac{R}{q_1^{m_1}}$, and $\pi_1'\lambda_1 : \frac{R}{(p_1^{n_1})} \to \frac{R}{q_1^{m_1}}$ is isomorphism.

Let $h : \frac{R}{(p_2^{n_2})} \oplus ... \oplus \frac{R}{(p_s^{n_s})} \to \frac{R}{(q_2^{m_2})} \oplus ... \oplus \frac{R}{q_r^{m_r}}$, $\lambda : B := \sum_{i=2}^{s} \oplus \frac{R}{p_i^{n_i}} \to \sum_{i=1}^{s} \oplus \frac{R}{p_i^{n_i}}$, $\pi : \sum_{i=1}^{r} \oplus \frac{R}{q_i^{m_i}} \to \sum_{i=2}^{r} \oplus \frac{R}{q_i^{m_i}} := B'$, let $h = (1 - \lambda_1'\pi_1')|_B : B \to B'$, $\forall v' \in B'$, $v' = \lambda_1'\pi_1'\lambda_1\theta_1^{-1}\pi_1(v') + (v' - \lambda_1'\pi_1'\lambda_1\theta_1^{-1}\pi_1(v'))$. Thus $\pi_1(v) = \pi_1(v') - \pi_1(v') = 0 \Rightarrow v \in B$, hence $v' = h(v') = (1 - \lambda_1'\pi_1')\lambda_1'\pi_1'\lambda_1\theta_1^{-1}\pi_1(v') + h(v) = h(v)$, h is surjective. $\forall v \in B \subseteq kerh$, $(v - \lambda_1'\pi_1'(v)) = 0 \Rightarrow v = \lambda_1'\pi_1'(v) \Rightarrow \pi_1\lambda_1'\pi_1'(v) = \pi_1(v) = 0 (\because v \in B)$, since $\theta_1 = \pi_1\lambda_1'\pi_1'\lambda_1$ and $\pi_1'\lambda_1$ are isomorphism, $\pi\lambda_1'$ is injective $\Rightarrow \pi_1'(v) = 0$, $v = \lambda_1'\pi_1'(v) = 0$

As known before that $\frac{R}{(p_i^{n_i})} \to \frac{R}{(q_i^{m_i})}$ is isomorphism, thus remove i, define $\varphi : \frac{R}{(p^n)} \xrightarrow{iso} \frac{R}{(q^m)}$, then prove $Rp = Rq$, $m = n$. As φ is surjective, $\therefore \exists a + (p^n) \in \frac{R}{(p^n)}$ s.t. $\varphi(a + (p^n)) = 1 + (q^m)$, $p^n\varphi(a + (p^n)) = p^n(1 + (q^m)) = p^n + (q^m)$, and $p^n\varphi(a + (p^n)) = \varphi(p^n a + (p^n)) = \varphi(0) = 0 + (q^m)$, $\therefore p^n \in (q^m) = Rq^m$, $\therefore p^n = rq^m$. On the other side, consider $\varphi^{-1} : \frac{R}{(q^m)} \to \frac{R}{(p^n)}$, similarly there is $q^m = sp^n$, thus $p^n = rq^m = rsp^n$, $\therefore rs = 1$, $p \mid p^n = r^q m \Rightarrow p \mid rq^m$, but p is prime, thus $p \mid r$ or $p \mid q$. If $p \mid r$, then $p \mid rs = 1 \Rightarrow 1 = xp$, but prime is irreversible, thus impossible. So $p \mid q$, $q = up$, $\therefore p^{n-1} = ruq^{m-1} \Rightarrow ... \Rightarrow 1 = ru^m q^{m-n} \Rightarrow m - n = 0$, $m = n$, $q \mid sp^n \Rightarrow q \mid p \Rightarrow p = vq \Rightarrow p = uvp \Rightarrow uv = 1$, $\therefore Rp = Rq$

Last but not the least, we need to prove when $1 = \theta_1 + ... + \theta_s$, then there is some θ_i that is isomorphism. $\theta_i = \pi_1\lambda_i'\pi_i'\lambda_1 : \frac{R}{(p_i^{n_i})} \to \frac{R}{(p_i^{n_i})}$ is R-module homomorphism, then remove the index i. Consider $End_R(\frac{R}{(p^n)}) : \{f : \frac{R}{(p_n)} \to \frac{R}{(p^n)}\ homomorphism\}$, define $\varphi : End_R(\frac{R}{(p^n)}) \to \frac{R}{(p^n)}$, $f \to f(1 + (p^n))$, then obviously φ is homomorphism. $\forall f \in ker\varphi$, $f(\bar{1}) = 0$, $\forall \bar{a} \in \frac{R}{(p^n)}$, $f(a + (p^n)) = f(a(1 + (p^n))) = af(\bar{1}) = a \cdot 0 = 0$, $\therefore f = 0$, φ is injective. $\forall \bar{a} \in \frac{R}{(p^n)}$, define $r_a \frac{R}{(p^n)} \to \frac{R}{(p^n)}$, $\bar{x} \to \overline{xa}$, $r_a \in End_R(\frac{R}{(p^n)})$, now $\varphi(ra) = a$, thus φ is surjective.

Thus $End_R(\frac{R}{(p^n)}) \cong \frac{R}{(p^n)}$, thus the ideal of the ring is $R(p^r + (p^n))$, because $\frac{R}{(p^n)}$ is irreducible. Consider $a'p^r + (p^n) \in \frac{R}{(p^n)}$, $p \not| a'$ is invertible means $\exists (b'p^s + (p^n))\ s.t.\ (b'p^s + (p^n))(a'p^r + (p^n)) = a'b'p^{r+s} + (p^n) = 1 + (p^n) \Rightarrow a'b'p^{r+s} - 1 = up^n \Rightarrow r = s = 0$(otherwise, $p \mid 1$). Thus $\theta_i = a_i p^{r_i} + (p^n)$, $p \not| a_i$, $\therefore \theta_1 + ... + \theta_s = (a_1 p^{r_1} + ... + a_s p^{r_s}) + (p^n)$, $\therefore \exists r_i = 0$(otherwise, $p \mid 1$). $\square$

Exercise .

We want to find the similar canonical form of a matrix$A = (a_{ij})_{n \times n}$, $F[x] \times F_A^n \to F_A^n$, as proved above, $F_A = \frac{F[x]}{(d_1(x))} \oplus ... \oplus \frac{F[x]}{(d_r(x))}$, in which $d_i(x) \mid d_{i+1}(x)$, and factorize $d_i(x)$, $d_i(x) = p_1^{e_{i1}} ... p_r^{e_{ir}}$, then $F_A = \sum_{j=1}^{r} \oplus \frac{F[x]}{(p_i(x)^{e_{ij}})}$, then choose a base on the new factorization form, we need to prove the existence and uniqueness of the similar canonical form.

Theorem .

$\forall A = (a_{ij})_{m \times n}$, $a_{ij} \in R$, R is PID, $UAV = diag(d_1, ..., d_r, 0, ..., 0), d_i \mid d_{i+1}$, U,V invertible, and$U'AV' = diag(d_1', ..., d_s', 0, ..., 0), d_i' \mid d_{i+1}'$, U',V' invertible, then $Rd_i = Rd_i'$ and s=r.