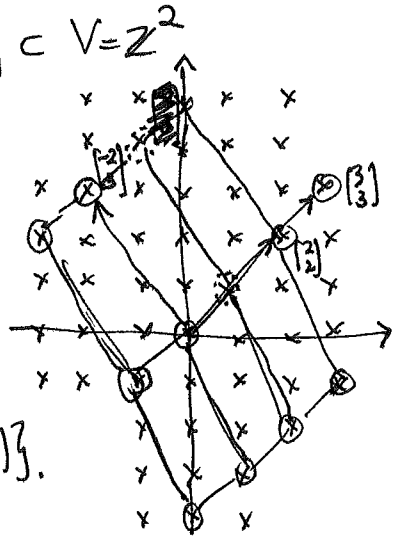
5/1/2019 (112)

③ The $\mathbb{Z}$-submodule $V' = \text{span}_{\mathbb{Z}}\left\{\begin{bmatrix}2\\2\end{bmatrix}, \begin{bmatrix}3\\3\end{bmatrix}, \begin{bmatrix}-2\\3\end{bmatrix}\right\} \subset V = \mathbb{Z}^2$



is free of rank 2, with $\mathbb{Z}$-basis $\left\{\begin{bmatrix}1\\1\end{bmatrix}, \begin{bmatrix}-2\\3\end{bmatrix}\right\}$:

They will be $\mathbb{Z}$-linearly independent because they are $\mathbb{R}$-linearly independent (why?)

and $\text{span}_{\mathbb{Z}}\left\{\begin{bmatrix}1\\1\end{bmatrix}, \begin{bmatrix}-2\\3\end{bmatrix}\right\} = \text{span}_{\mathbb{Z}}\left\{\begin{bmatrix}2\\2\end{bmatrix}, \begin{bmatrix}3\\3\end{bmatrix}, \begin{bmatrix}-2\\3\end{bmatrix}\right\}$.

One also has quotient modules and Noether's 1st iso. thm...

DEFIN: Given an R-submodule $V' \subset V$, the quotient $V/V' = \{v + V' : v \in V\}$ becomes an R-module with usual $+$ and R-scaling by $r(v+V') := rv + V'$

$(v_1+V') + (v_2+V') := v_1+v_2+V'$

PROPOSITION: Given an R-module homomorphism $V_1 \xrightarrow{\varphi} V_2$

- $\ker\varphi \subset V_1$ is an R-submodule ($= \varphi^{-1}(0)$)
- $\text{im}\varphi \subset V_2$ is an R-submodule
- if $V' \subset \ker\varphi$ is an R-submodule, then φ induces a homomorphism $V_1/V' \xrightarrow{\bar{\varphi}} V_2$ via $v_1 + V' \longmapsto \bar{\varphi}(v_1+V') := \varphi(v_1)$
- if $V' = \ker\varphi$, this becomes an isomorphism $V_1/\ker\varphi \xrightarrow{\bar{\varphi}} \text{im}\varphi$

proof: All straightforward, just checking the R-scaling is respected in each case ∎

OUR plan:

① For free R-modules, show homoms $R^n \xrightarrow{\varphi} R^m$ are always multiplication by a matrix $A \in R^{m\times n}$ i.e. $\underline{x} = \begin{bmatrix}x_1\\\vdots\\x_n\end{bmatrix} \longmapsto A\underline{x}$

② For the class of Noetherian rings R (including PID's), show finitely generated R-modules M are all of the form $R^m/\text{im}\varphi$ where $R^n \xrightarrow{\varphi} R^m$ is a homom. $= R^m/\text{im}A$

③ For PID's R, show $\exists$ change-of-bases in R^n, R^m making $A = \begin{bmatrix}d_1 & & & 0\\ & \ddots & & \\ & & d_r & \\ 0 & & & 0\end{bmatrix}$ with $d_i \in R$, so $M \cong R^m/\text{im}A \cong R^{m-r} \oplus R/(d_1) \oplus \cdots \oplus R/(d_r)$

Let's deal with these in the order ①, ③, ②.

PROPOSITION: Any R-module homom. $R^n \xrightarrow{\varphi} R^m$ is of the form $\underline{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \mapsto \varphi(\underline{x}) = A\underline{x}$ where $A \in R^{m\times n}$ (a_{ij}) is defined by $\varphi(e_j) \overset{(*)}{=} \sum_{i=1}^{m} a_{ij} e_i$ (with $e_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \leftarrow i^{th}$ entry)

proof: Usual proof: if $(*)$ defines A, then

$$\varphi(\underline{x}) = \varphi(x_1 e_1 + \dots + x_n e_n) = x_1\varphi(e_1) + \dots + x_n \varphi(e_n) = \sum_{j=1}^{n} x_j \varphi(e_j)$$

$$= \sum_{j=1}^{n} x_j \sum_{i=1}^{m} a_{ij} e_i = \sum_{i=1}^{m} (A\underline{x})_i e_i$$

$$= A\underline{x} \quad \blacksquare$$

Sometimes we want to change bases in R^n, R^m to make the matrix A for φ look simpler, by applying P, Q that are square and invertible $n\times n$, $m\times m$.

PROPOSITION: $P \in R^{n\times n}$ is invertible in $R^{n\times n}$, i.e. $P \in GL_n(R)$,

$$\iff \det P \in R^\times$$

proof: ($\Rightarrow$): If $P^{-1} \in R^{n\times n}$ exists, then $P \cdot P^{-1} = I_n$

$$\Downarrow$$

$$\det(P \cdot P^{-1}) = \det(I_n) \quad \Rightarrow \det P \in R^\times$$

$$\Vert \qquad\qquad \Vert$$

$$\det P \cdot \det(P^{-1}) \qquad 1$$

$$\in R \qquad \in R$$

need the identity $\det(A\cdot B) = \det A \cdot \det B$ for $A, B \in R^{n\times n}$

($\Leftarrow$): If $\det P \in R^\times$, then using the identity $\boxed{P \cdot \operatorname{cof}(P) = \det P \cdot I_n}$

where $\operatorname{cof}(P) \in R^{n\times n}$ has $\operatorname{cof}(P)_{i,j} = (-1)^{i+j} \det\left(P - \{j^{th} \text{ row}, i^{th} \text{ col}\}\right)$, one has $P^{-1} = (\det P)^{-1} \cdot \operatorname{cof}(P)$ $\in R^{n\times n}$ $\blacksquare$

EXAMPLES: ① $P \in \mathbb{Z}^{n\times n}$ lies in $GL_n(\mathbb{Z}) \Leftrightarrow \det P \in \mathbb{Z}^\times = \{+1,-1\}$

e.g. $P=\begin{bmatrix}2&5\\1&3\end{bmatrix}$ has $\det P = 2\cdot 3 - 1\cdot 5 = 1$, and $P^{-1}=\begin{bmatrix}3&-5\\-1&2\end{bmatrix}$ in $GL_2(\mathbb{Z})$

but $P=\begin{bmatrix}2&5\\1&4\end{bmatrix}$ has $\det P = 2\cdot 4 - 1\cdot 5 = 3 \notin \mathbb{Z}^\times$, so $P \notin GL_2(\mathbb{Z})$

② $P \in \mathbb{F}[x]^{n\times n}$ ($\mathbb{F}$ a field) lies in $GL_n(\mathbb{F}[x]) \Leftrightarrow \det P \in \mathbb{F}^\times \ (= \mathbb{F}[x]^\times)$

e.g. $P=\begin{bmatrix}x&x-2\\x+2&x\end{bmatrix}$ has $\det P = x^2-(x^2-4)=4 \in \mathbb{Q}^\times$,

$\in \mathbb{Q}[x]^{2\times 2}$ and $P^{-1}=\frac{1}{4}\begin{bmatrix}x&-x+2\\-x-2&x\end{bmatrix}$

REMARK (§14.3): Do identities like $\det(AB)=\det A\cdot\det B$

$A\cdot \mathrm{cof}(A) = \det A \cdot I_n$ still hold for $A,B\in R^{n\times n}$ with any ring R?

Yes, because we proved them when R is any field $\mathbb{F}$,

even one like $\mathbb{F}=\mathbb{Q}(a_{11},a_{12},\dots,a_{nn},b_{11},b_{12},\dots,b_{nn})$ with a_{ij},b_{ij} as variables,

so they also hold in $\mathbb{Z}[a_{11},a_{12},\dots,a_{nn},b_{11},b_{12},\dots,b_{nn}]$ $\cup$ subring

and then one can apply a ring (substitution) homomorphism

$$\mathbb{Z}[a_{ij},b_{ij}] \longrightarrow R$$

$a_{ij} \longmapsto (i,j)$ entry of A

$b_{ij} \longmapsto (i,j)$ entry of B

to see that they hold for any R.