(118) To show PID's R have all fin. gen'd modules $M = R^m/\mathrm{im}A$, need a key idea of Noether.

DEF'N/PROPOSITION: The following are equivalent for an R-module M, and define M being a Noetherian R-module:

(i) $\nexists$ R-submodules $\overbrace{M_1 \subsetneq M_2 \subsetneq \cdots}^{\infty \text{ sequence}}$ $(\subset M)$
(the ascending chain condition or ACC on submodules)

(ii) every R-submodule $N \subseteq M$ is finitely generated.

proof: (i)$\Rightarrow$(ii): Assuming the ACC, if $N \subseteq M$ is a submodule, either $N = \{0\}$ and we're done since $N = \mathrm{span}_R(\emptyset)$, or $\exists\, n_1 \neq 0$ in N and maybe we're done with $N = \mathrm{span}_R(\{n_1\}) = Rn_1$ or $\exists\, n_2 \in N - Rn_1$ and maybe we're done with $N = \mathrm{span}_R(\{n_1, n_2\}) = Rn_1 + Rn_2$

$\vdots$

This must terminate, else $Rn_1 \subsetneq Rn_1 + Rn_2 \subsetneq \cdots$ is an infinite ascending chain of submodules.
(with $N = Rn_1 + Rn_2 + \cdots + Rn_t$)

5/5/2019 > (ii)$\Rightarrow$(i): Assuming (ii), given an ascending chain

$$M_1 \subseteq M_2 \subseteq \cdots \subset M,$$

let $N := \bigcup_{i=1}^{\infty} M_i$, and check that is an R-submodule (easy) so finitely generated by (ii) as $N = Rn_1 + \cdots + Rn_t$

and each $n_i \in M_{f(i)}$ for $i = 1, 2, \ldots, t$,
so $N \subseteq M_{i_0}$ where $i_0 = \max\{f(1), f(2), \ldots, f(t)\}$
and $M_{i_0} = M_{i_0+1} = \cdots$ ∎

How to use this?

DEF'N: A ring R is a Noetherian ring if it is Noetherian as an R-module,
i.e. (i) $\nexists$ ideals $I_1 \subsetneq I_2 \subsetneq \cdots \subset R$
or equivalently (ii) every ideal $I \subset R$ is fin. gen'd, i.e. $I = Rr_1 + \cdots + Rr_t = (r_1, \ldots, r_t)$ for some $r_1, \ldots, r_t \in R$

(119)

EXAMPLES: (§14.6)

① PID's R are Noeth. rings since ~~they~~ ideals I are principal: $I=(r)$ for some $r\in R$. E.g. $\mathbb{Z}$, $\mathbb{F}[x]$ are Noetherian.

② Hilbert's basis theorem (which we won't prove and don't need here) (Thm 14.6.7) says R Noeth. $\Rightarrow R[x]$ Noeth.

so $\mathbb{Z}[x]$, $\mathbb{F}[x,y]$
$\mathbb{Z}[x,y]$, $\mathbb{F}[x_1,x_2,\ldots,x_n]$
$\mathbb{Z}[x_1,x_2,\ldots,x_n]$
are all Noetherian.

③ Not hard to see quotients of Noeth. rings are Noeth. (but don't need it)

THEOREM (14.6.5, 14.6.6)

(a) Given a R-module homomorphism $V \xrightarrow{\varphi} V'$, if both $\ker\varphi \subset V$, $\operatorname{im}\varphi \subset V'$ are Noetherian R-modules, then so is V.

(b) For a Noetherian ring R, every finitely gen'd R-module V is a Noetherian R-module.

proof: (a): Given a submodule $U \subset V$ consider the restriction $\varphi|_U$ of φ to U and

$$\ker(\varphi|_U) \subset \ker\varphi$$
$$\operatorname{im}(\varphi|_U) = \varphi(U) \subset \operatorname{im}\varphi = \varphi(V)$$

which must both be finitely gen'd R-modules, since $\ker(\varphi), \operatorname{im}(\varphi)$ are Noetherian. So let $u_1,\ldots,u_t$ generate $\ker(\varphi|_U)$ and $\varphi(u_{t+1}),\ldots,\varphi(u_s)$ generate $\operatorname{im}(\varphi|_U)$,

and we claim $u_1,\ldots,u_t,u_{t+1},\ldots,u_s$ generate U:

any $u\in U$ has $\varphi(u) = r_{t+1}\varphi(u_{t+1})+\ldots+r_s\varphi(u_s)$ for some $r_{t+1},\ldots,r_s\in R$

$$= \varphi(r_{t+1}u_{t+1}+\ldots+r_su_s)$$

so $\varphi(u-(r_{t+1}u_{t+1}+\ldots+r_su_s)) = 0$

i.e. $u - \sum_{j=t+1}^{s} r_ju_j \in \ker(\varphi|_U)$, so $u - \sum_{j=t+1}^{s} r_ju_j = r_1u_1+\ldots+r_tu_t$ for some $r_1,\ldots,r_t$

$\Rightarrow u \in \operatorname{span}\{u_1,\ldots,u_t,u_{t+1},\ldots,u_s\}$.

(b): First show a Noeth. ring R has R^n a Noeth. R-module via induction on n, in which the base case $n=1$ is by definition since $R^1 \cong R$ and the inductive step follows by applying (a) to this homom.

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \\ x_n \end{bmatrix} \in R^n \xrightarrow{\varphi} R \ni x_1$$

with $\mathrm{im}(\varphi) = R$ a Noeth. R-module

$\ker(\varphi) = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_{n-1} \\ 0 \end{bmatrix} \in R^n \right\} \cong R^{n-1}$ a Noeth. R-module by induction.

Then any finitely gen'd R-module V spanned by $\{v_1, \ldots, v_n\}$ has a surjective homom. $R^n \xrightarrow{\varphi} V$.

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \longmapsto x_1 v_1 + \ldots + x_n v_n$$

So an R-submodule $V' \subset V$ will have $\varphi^{-1}(V') \subset R^n$ an R-submodule, which must be finitely gen'd since R^n is Noeth., say by $u_1, \ldots, u_t \in \varphi^{-1}(V') \subset R^n$ and then $\varphi(u_1), \ldots, \varphi(u_t) \in V'$ will generate V'.

THEOREM: (a) For a Noeth. ring R, every fin. gen'd R-module $V \cong R^m / \mathrm{im} A$ for some $R^n \xrightarrow{A} R^m$, $A \in R^{m \times n}$.

(b) If R is a PID, $V \cong R/(d_1) \times \ldots \times R/(d_r) \times R^{m-r}$

(c) — " —, one can assume each $d_i = p_i^{e_i}$ for some ~~prime~~ irreducible in R

proof: (a) V fin. gen'd by $v_1, \ldots, v_m \Rightarrow R^m \xrightarrow{\varphi} V$ has $V = \mathrm{im}\,\varphi \cong R^m / \ker \varphi$

$$\begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix} \longmapsto x_1 v_1 + \ldots + x_m v_m$$

and $\ker \varphi \subset R^m$ must be fin. gen'd (since R^m Noeth.) say by $u_1, \ldots, u_n \in R^m$, that one can write as $u_j = \sum_{i=1}^{m} a_{ij} e_i$, i.e. $A = \begin{bmatrix} | & & | \\ u_1 & \cdots & u_n \\ | & & | \end{bmatrix}$

Then $\ker \varphi = \mathrm{im} A$ where $A = (a_{ij})$, and $V \cong R^m / \ker \varphi = R^m / \mathrm{im} A$.

(b) Find $S = Q^{-1} A P = \left[\begin{array}{c|c} \begin{matrix} d_1 & 0 \\ 0 & d_r \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right]$ by Smith normal form algorithm.

(c) Given $d \in R$ a PID that factors $d = p_1^{e_1} \cdots p_s^{e_s}$, p_i irred./prime,

repeatedly use <u>SunZe's Thm:</u> If $d = ab$ with $\gcd(a,b) = 1$ in a PID R,

$$\text{then } R/(d) \cong R/(a) \times R/(b)$$
$$\text{via } \bar{r} \overset{f}{\longmapsto} (\bar{r}, \bar{r})$$

<u>proof:</u> f is injective since $f(\bar{r}) = (\bar{0}, \bar{0}) \Rightarrow a, b$ divide r
$\Rightarrow \underset{\overset{\shortparallel}{d}}{ab}$ divides r
$\Rightarrow \bar{r} = 0$

f is surjective since if $ax + by = 1$ for $x, y \in R$
then any $(\bar{c}, \bar{d}) \in R/(\bar{a}) \times R(\bar{b})$
has $f(cby + dax) = (\overline{cby + dax}, \overline{cby + dax})$
$= (\overline{cby}, \overline{dax})$
$= (\bar{c}, \bar{d})$ ∎

<u>COROLLARY:</u> Fin. gen'd abelian groups (= $\mathbb{Z}$-modules) are all of form $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z} \times \mathbb{Z}^{m-r}$
(§14.7)

and <u>finite</u> ones are of form $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$

<u>COROLLARY:</u> Every $\mathbb{C}$-linear transformation $\mathbb{C}^n \xrightarrow{A} \mathbb{C}^n$, $A \in \mathbb{C}^{n \times n}$
(§14.8)
can be brought by a change-of-basis ($P \in GL_n(\mathbb{C})$) to Jordan form

$$P^{-1}AP = \begin{bmatrix} J_1 & & & 0 \\ & J_2 & & \\ & & \ddots & \\ 0 & & & J_r \end{bmatrix} \text{ where each } J_i = \begin{bmatrix} \lambda_i & 1 & & 0 \\ & \lambda_i & 1 & \\ & & \ddots & 1 \\ 0 & & & \lambda_i \end{bmatrix} \text{ or } \begin{bmatrix} \lambda_i & & 0 \\ 1 & \ddots & \\ 0 & 1 & \lambda_i \end{bmatrix}$$

<u>proof:</u> $V = \mathbb{C}^n$ is a $\mathbb{C}[x]$-module via $x(v) = Av$, fin. gen'd by $e_1, \ldots, e_n$,

$$\text{so } V \cong \mathbb{C}[x]/(\underbrace{p_1(x)}_{\substack{p_1(x) \text{ irred. in } \mathbb{C}[x] \\ = x - \lambda_1}}{}^{e_1}) \times \cdots \times \mathbb{C}[x]/(\underbrace{p_r(x)}_{\substack{p_r(x) \text{ irred.} \\ = x - \lambda_r}}{}^{e_r}) \times \underbrace{\cancel{\mathbb{C}[x]^{m-r}}}_{\text{infinite dimensional over } \mathbb{C}!}$$

(122)

So $\exists P \in GL_n(\mathbb{C}[x]) = GL_n(\mathbb{C})$ with $P^{-1}AP = \begin{bmatrix} \boxed{J_1} & & O \\ & \boxed{J_2} & \\ O & & \ddots \; \boxed{J_r} \end{bmatrix}$

where J expresses the x acting on $\underbrace{\mathbb{C}[x]/((x-\lambda)^e)}_{\substack{\mathbb{C}\text{-basis: } \{1, x, x^2, \ldots, x^{e-1}\} \\ \text{or } \{1,\, x-\lambda,\, (x-\lambda)^2, \ldots, (x-\lambda)^{e-1}\}}}$ for some $\lambda \in \mathbb{C}$

i.e. $$J = \begin{array}{c} \\ 1 \\ (x-\lambda) \\ (x-\lambda)^2 \\ \vdots \\ \\ (x-\lambda)^{e-1} \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & (x-\lambda) & (x-\lambda)^2 & \cdots & (x-\lambda)^{e-1} \end{array} \\ \begin{bmatrix} \lambda & 0 & 0 & \cdots & 0 & 0 \\ 1 & \lambda & 0 & & \vdots & \vdots \\ 0 & 1 & \lambda & & \vdots & \vdots \\ \vdots & 0 & 1 & \ddots & 0 & \vdots \\ \vdots & \vdots & 0 & & \lambda & 0 \\ 0 & 0 & 0 & & 1 & \lambda \end{bmatrix} \end{array}$$

since

$(x-\lambda)(x-\lambda)^i = (x-\lambda)^{i+1}$

$\Downarrow$

$x(x-\lambda)^i = 1\cdot(x-\lambda)^{i+1} + \lambda(x-\lambda)^i$

$\blacksquare$