FRI, Nov 21, 2014

Last time:

Thm Let R be a PID, M finitely generated. Then $\exists$

$p_i \in R$ primes, $i = 1, \dots, k$

$n_i \in \mathbb{Z}_{\geq 1}$, $i = \phi, \dots, k$, $n_0 \in \mathbb{Z}_{\geq 0}$,

s.t.

$$M \cong \bigoplus_{i=1}^{k} R/(p_i^{n_i}) \oplus R^{n_0}.$$

$$\cong R^{n_0} \oplus R/(p_1^{n_1}) \oplus R/(p_2^{n_2}) \oplus \cdots \oplus R/(p_k^{n_k}).$$

Rmk We allow $p_i = p_j$ for $i \neq j$.

Exer Classify all abelian gps of order

$$7 \cdot 7 \cdot 11 \cdot 11 = 5929.$$

Pf Need to find all combinations of p_i, n_i such that

$$5929 = \left| \mathbb{Z}/(p_1^{n_1}) \oplus \cdots \oplus \mathbb{Z}/(p_k^{n_k}) \right|$$

$$= p_1^{n_1} \cdot \cdots \cdot p_k^{n_k}.$$

	(p_1, n_1)	(p_2, n_2)	(p_3, n_3)	(p_4, n_4)
$\mathbb{Z}/49\mathbb{Z} \oplus \mathbb{Z}/121\mathbb{Z}$	$(7,2)$	$(11,2)$	—	—
$\mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/121\mathbb{Z}$	$(7,1)$	$(7,1)$	$(11,2)$	—
$\mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/11\mathbb{Z} \oplus \mathbb{Z}/11\mathbb{Z}$	$(7,1)$	$(7,1)$	$(11,1)$	$(11,1)$
$\mathbb{Z}/49\mathbb{Z} \oplus \mathbb{Z}/11\mathbb{Z} \oplus \mathbb{Z}/11\mathbb{Z}$	$(7,2)$	$(11,1)$	$(11,1)$	—

$$\boxed{\text{Note: } \mathbb{Z}/p^2\mathbb{Z} \not\cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}\,!}$$

Exer Which of these is $\mathbb{Z}/5929\mathbb{Z}$ isomorphic to?

Ans: You showed $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$ if $\gcd(m,n)=1$.

So $$\mathbb{Z}/49\mathbb{Z} \oplus \mathbb{Z}/121\mathbb{Z} \cong \mathbb{Z}/5929\mathbb{Z}.$$

Recall: Let F be a field, and let V be a F vector space. (This just means V is a module over F.) Then any

$$A : V \to V, \quad F\text{-linear map,}$$

defines a $F[t]$-module structure on V:

If $f = a_d t^d + \cdots + a_1 t + a_0$,

$$f v := a_d A^d(v) + \cdots + a_1 A(v) + a_0 v.$$

where

$$A^i = \underbrace{A \circ \cdots \circ A}_{i \text{ times}}.$$

So let V be a fin-dim vector space over F. Fix an F-linear $A: V \to V$ to make V an $F[t]$-module.

<u>Prop</u> V is finitely generated as an $F[t]$-module.

<u>Pf</u>. Let $v_1, \dots, v_n$ be a finite basis. Then

$$V = \{ b_1 v_1 + \cdots + b_n v_n \mid b_1, \dots, b_n \in F \}.$$

In particular, if $f_i = b_i$ are constant polynomials,

$$V = \{ f_1 v_1 + \cdots + f_n v_n \}$$

so the function

$$\begin{aligned} F[t] \oplus \cdots \oplus F[t] &\longrightarrow V \\ e_i &\longmapsto v_i \end{aligned}$$

is a surjection. //

<u>Cor</u> V is isomorphic (as an $F[t]$-module) to

$$F[t]/(p_1^{n_1}) \oplus \cdots \oplus F[t]/(p_k^{n_k}) \oplus F[t]^{n_0}$$

for $p_i \in F[t]$ irreducible, $n_i \geq 1$, $n_0 \geq 0$.

<u>Rmk</u> $n_0 = 0$; why? V is a fin-dim vec space over F, but $F[t]$ isn't, so V couldn't contain a subspace $\cong$ to $F[t]$.

In general, identifying irreducible polynomials can be hard:
For instance, when is $x^3 + 2x^2 + x + 1$ irreducible over $\mathbb{Z}/p\mathbb{Z}$?
We'd probably check case by case.

Defn F is called <u>algebraically</u> <u>closed</u> if every non-constant polynomial $f \in F[t]$ admits a root.

Ex $\mathbb{C}$ is algebraically closed.

Thm (Next semester?) Any field F admits an ~~injection into~~ injective ring homom. into an alg. closed field.

Rmk Not trivial — sure, $\mathbb{R} < \mathbb{C}$, but how about $\mathbb{Z}/_p\mathbb{Z}$?

Prop If F is alg. closed, $f \in F[t]$ is irreducible iff f is linear. (ie, $f = a_1 t + a_0$, $a_1 \neq 0$).

Pf $\deg f \geq 2 \Rightarrow f$ can be factored by linear poly since f has a root.
$\Rightarrow f$ not irred.
We saw last time every deg 1 poly is irred in any field. //

Cor If F is algebraically closed and V is a fin-dim vec space w/ $A: V \to V$ F-linear, then

$$V \cong F[t]/(t-\alpha_1)^{n_1} \oplus \cdots \oplus F[t]/(t-\alpha_k)^{n_k}$$

for some $\alpha_i \in F$.

Rmk If $f = a_1 t - a_0$, then $a_1^{-1} f = t - a_1^{-1} a_0$, (assuming $a_1 \neq 0$) so $(f) = (a_1^{-1} f) = (t - a_1^{-1} a_0)$. That is, we can always assume $a_1 = 1$.

Let's see some examples: We want to study

$$F[t]/(t-\alpha)^n$$

as a F-module, and as an $F[t]$-module.

(Note the $F[t]$-module structure on $F[t]/(p^n)$ is

$$\begin{aligned} F[t] \times F[t]/(p^n) &\longrightarrow F[t]/(p^n) \\ (f, \bar{g}) &\longmapsto (\overline{fg}). \end{aligned}$$
)

1

Prop'n If $\deg p = d$,

$$F[t]/(p^n) \cong F^{n \cdot d}$$

as a F-vector space.

Pf.: Any $f \in F[t]$ can be written $f = p^n \cdot q + r$ where $\deg r < \deg p^n = nd$.

Since r, q are unique given p^n, f the function

$$\bar{f} \longmapsto r, \quad F[t]/(p^n) \longrightarrow \{\text{polyn of degree} \leq nd-1\} \cong F^{nd}$$

gives a bijection. //

Ex

$$V = F[t]/(t) \,. \qquad \alpha = 0, \quad n = 1$$

What is $F[t]$-action?

(1) $F[t]/(t) \cong \{\text{constant polyn}\}$

$\cong F$.

~~(2) $t \cdot a_0 = (a_0 t) =$~~

(2) $t \cdot \overline{a_0} = \overline{t a_0} = \overline{0}$ since $a_0 t \in (t)$.

i.e., multiplication by $t \longleftrightarrow A : F \to F$,
$a_0 \mapsto 0$

Ex $V = F[t]/(t - \alpha)$. Mult. by $t \longleftrightarrow A : V \longrightarrow V$

$$\overline{a_0} \longmapsto \overline{t a_0} = \overline{(t-\alpha) a_0} + \alpha \overline{a_0} = \alpha \overline{a_0}.$$

i.e., $A : F \longrightarrow F$
$a_0 \mapsto \alpha a_0$.

<u>Ex</u> Let

$$V = F[t]/(t-\alpha)^n.$$

Then V has a basis

$$\underset{\underset{V_0}{\shortparallel}}{\overline{1}}, \quad \underset{\underset{V_1}{\shortparallel}}{\overline{t-\alpha}}, \quad \overline{(t-\alpha)^2}, \quad \cdots, \quad \underset{\underset{V_{n-1}}{\shortparallel}}{\overline{(t-\alpha)^{n-1}}}.$$

Moreover,

$$\begin{aligned} t\,V_i = t\,\overline{(t-\alpha)^i} &= (t-\alpha)\overline{(t-\alpha)^i} + \alpha\overline{(t-\alpha)^i} \\ &= \overline{(t-\alpha)^{i+1}} + \alpha\overline{(t-\alpha)^i} \\ &= V_{i+1} + \alpha V_i \end{aligned}$$

So

$$A = \begin{pmatrix} \alpha & 1 & & & \\ & \alpha & 1 & & 0 \\ 0 & & \alpha & 1 & \\ & & & \ddots & 1 \\ & & 0 & & \alpha \end{pmatrix} \quad \begin{array}{l} \alpha \text{ on diag,} \\ 1 \text{ right above diag.} \end{array}$$