PART C

Group algebras and modules over p-local rings

§14. Discrete valuation rings

classical theory: representations in char 0 (Schur, Frobenius)
modular theory: represetations in char p (Brauer 1930)

connection between char 0 and char $p > 0$:
<u>p-local rings</u> whose quotient by the max ideal is of char p and whose field of fractions is of char zero.

<u>Roughly speaking:</u>

$\mathcal{O}$ a comm, local ring , $J(\mathcal{O})$ - max ideal
$k := \mathcal{O}/J(\mathcal{O})$ of char $p > 0$
$K := Q(\mathcal{O})$ of char 0
$(K, \mathcal{O}, k)$ - p-modular system

$$\begin{array}{ccc} \mathcal{O}G & \hookrightarrow & KG \\ \downarrow & & \\ kG & & \end{array} \qquad \begin{array}{ccc} \mathrm{Mod}(\mathcal{O}G) & \longrightarrow & \mathrm{Mod}(KG) \\ & M & \longmapsto K \otimes_{\mathcal{O}} M \\ \downarrow & \downarrow & \\ \mathrm{Mod}(kG) & k \otimes_{\mathcal{O}} M & \end{array}$$

Recall: A comm. ring $\mathcal{O}$ is called <u>local</u> if it has a unique maximal ideal. In particular the Jacobson radical $J(\mathcal{O})$ is this maximal ideal.

Ex: 1. $\mathbb{Z}_{(p)} = \{\frac{a}{b},\ a, b \in \mathbb{Z}, (b,p) = 1\}$
is local with max ideal $p \cdot \mathbb{Z}_{(p)}$.
2. kP, P finite p-group k - field of char p,
is local: $I(kP) = J(kP)$ is the maximal ideal.

Prop 1 $\mathcal{O}$ commutative. Then $\mathcal{O}$ is local iff
$\mathcal{O}^\times = \mathcal{O} \setminus J(\mathcal{O})$.

Proof:

- $\mathcal{O}^\times = \mathcal{O} \setminus J(\mathcal{O}) \Rightarrow J(\mathcal{O})$ is maximal $\Rightarrow J(\mathcal{O})$ is the unique max ideal of $\mathcal{O}$.
- $J(\mathcal{O})$ is the unique max ideal then $\mathcal{O}/J(\mathcal{O}) \simeq k$ a field
take $\lambda \in \mathcal{O} \setminus J(\mathcal{O})$ then $\bar{\lambda} \neq 0$ in k, so $k = \cancel{k}\bar{\lambda}$
But then $\mathcal{O} = \mathcal{O}\lambda + J(\mathcal{O})$. By Nakayama
$\mathcal{O} = \mathcal{O}\lambda$ and hence $\lambda \in \mathcal{O}^\times$.

Prop 2 Let $\mathcal{O}$ be commutative local Noeth ring.
Then $\bigcap_{k \geq 1} J(\mathcal{O})^k = \{0\}$.

Proof:
We have that $N = \bigcap_{k \geq 1} J(\mathcal{O})^k$ is fin. generated as $\mathcal{O}$ is Noetherian. Aim: $J(\mathcal{O}) N = \cancel{J(\mathcal{O})}\ N$

1) $\exists\ U$ an ideal of $\mathcal{O}$ maximal such that $\cancel{J(\mathcal{O})}\ N \cap U = J(\mathcal{O}) N$
(U exists by Zorn, as $\mathcal{O}$ is Noetherian)
2) $\lambda \in J(\mathcal{O})$, then $\lambda^n \in U$ for some $n \geq 0$
Let $U_k = \{\mu \in \mathcal{O} \mid \mu \lambda^k \in U\}$. Then $U_k \subseteq U_{k+1}$
and because $\mathcal{O}$ is Noetherian, $\exists m$, $U_m = U_{m+1}$
Now $J(\mathcal{O}) N = N \cap U \subseteq N \cap (U + \lambda^m \mathcal{O})$
to see that this is "="

Soit $\alpha \in (U + \lambda^m \Theta) \cap N$

$\Rightarrow \alpha = u + \lambda^m \mu \in N$

Then $\lambda\alpha = \lambda u + \lambda^{m+1}\mu \in J(\Theta) N \subseteq U$

$\Rightarrow \lambda^{m+1}\mu \in U$ so $\lambda^m \mu \in U$ (as $U_m = U_{m+1}$)

$\Rightarrow \mu \in U_{m+1} = U_m$

$\Rightarrow \alpha = u + \lambda^m \mu \in U \cap N$ and $U \cap N = (U + \lambda^m \Theta) \cap N$

But U is maximal with this property so $\lambda^m \in U$.

3) Θ is Noetherian $\Rightarrow J(\Theta)$ is finitely generated. $J(\Theta) = \sum \Theta \lambda_i$. Moreover by 2) there exists m_i such that $\lambda_i^{m_i} \in U$.

Take $m := \max\{m_i : i = 1, \dots, n\}$

Then $N \subseteq J(\Theta)^{mn} \subseteq \sum_i \Theta \lambda_i^m \subseteq U$

only place where one uses the definition of N

Thus $J(\Theta) N = U \cap N = N$ and by Nakayama's lemma $N = \{0\}$.

□

Thm 3 Θ a comm local Noeth ring. Then every fin. generated proj Θ-module is free.

Proof: Let M be a proj, fin. gen Θ-mod. Take $k := \Theta / J(\Theta)$ a field. Thus $M / J(\Theta) M$ is a k-vector space and a fin. dim. one.

$$\begin{tikzcd} \Theta^n \arrow[r, "\alpha"] \arrow[d] \arrow[dr, phantom, "\circlearrowright"] & M \arrow[d] \\ k^n \arrow[r, "\sim"] & M/J(\Theta)M \end{tikzcd}$$

α exists as M is proj.

$\mathrm{Im}(\alpha) + J(\Theta) M = M$

$\Rightarrow \mathrm{Im}(\alpha) = M$

(α is surj)

$$\begin{tikzcd} \mathcal{O}^n \arrow[r, "\alpha"] & M \arrow[l, dashed, bend left, "\beta"] \end{tikzcd}$$, α - surj + M - proj

$\Rightarrow \alpha$ splits: $\exists\, \beta : M \to \mathcal{O}^n$

$\alpha \circ \beta = id_M$.

Now
$$\begin{tikzcd} \mathcal{O}^n \arrow[d] & M \arrow[l, "\beta"'] \arrow[d] \\ k^n \arrow[r, phantom, "\cong"] & M/J(\mathcal{O})M \end{tikzcd}$$

$Im(\beta) + J(\mathcal{O})^n = \mathcal{O}^n$

$\Rightarrow Im(\beta) = \mathcal{O}^n$

$\Rightarrow \alpha$ and β are inverses of each other and $M \cong \mathcal{O}^n$.

~~Def~~ We say that a comm, local, Noetherian ring $\mathcal{O}$ is <u>complete</u> if $\forall \{\lambda_i\}_{i\geq 1}$, $\lambda_{i+1} - \lambda_i \in J(\mathcal{O})^i$ there exists $(\lambda \in \mathcal{O})$ such that $\lambda - \lambda_i \in J(\mathcal{O})^i$ for $i >> 0$.

<u>Rem</u> : If λ exists, it is unique as $\bigcap_{k\geq 1} J(\mathcal{O})^k = \{0\}$.

<u>Thm 4</u>. $\mathcal{O}$ commutative, Noetherian, local. Then there exists $\hat{\mathcal{O}}$ comm, Noeth, local and complete and $\sigma : \underset{J(\mathcal{O}) \hookrightarrow J(\hat{\mathcal{O}})}{\mathcal{O} \longrightarrow \hat{\mathcal{O}}}$ with the univ. prop that $\forall\ \mathcal{O}'$ comm, Noeth, local and complete and $\sigma' : \underset{J(\mathcal{O}) \hookrightarrow J(\mathcal{O}')}{\mathcal{O} \longrightarrow \mathcal{O}'}$ there exists a unique ring homo $\tau : \hat{\mathcal{O}} \to \mathcal{O}'$ such that $\sigma' = \tau \circ \sigma$. In particular $(\hat{\mathcal{O}}, \sigma)$ is unique up to unique isom.

<u>Proof</u> : standard proof for the existence of a completed object (take all Cauchy seq.) The details are left in exercise

$\square$.

Def: a module M over a local comm, Noeth ring $\mathcal{O}$ is complete if for every $\{m_i\}_{1\leq i\leq n}$, $m_{i+1}-m_i \in \mathcal{J}(\mathcal{O})^i M$ there exists $m\in M$, $m-m_i\in \mathcal{J}(\mathcal{O})^i M$, $i \gg 0$. The element m is the limit of $\{m_i\}$ and it is unique as $\bigcap_{i\geq 1}\mathcal{J}(\mathcal{O})^i = \{0\}$.

Thm 5 Let $\mathcal{O}$ be complete, comm local Noeth ring. Then every fin gene $\mathcal{O}$-mod is complete.

Proof:

- $\mathcal{O}$ is complete as regular $\mathcal{O}$-module
- $\mathcal{O}^n$ is also complete, as being free $\mathcal{O}$-module.
- now if M is finitely generated as $\mathcal{O}$-module there is a surj morph $\mu: F \to M$

  let $(m_i)_{i\geq 1}$ be a Cauchy seq in M; $\mu(\alpha_1)=m_1$

  Take $\gamma_k \in F$ such that $\mu(\gamma_k)=m_{k+1}-m_k$.

  Define $\alpha_{k+1}=\alpha_k+\gamma_k$. In fact γ_k can be chosen in $\mathcal{J}(\mathcal{O})^k F$ and hence $(\alpha_k)_{k\geq 1}$ is a Cauchy sequence so it has a limit $\alpha\in F$

  One can easily prove that $\mu(\alpha)$ is the limit of $\{m_i\}_{i\geq 1}$ in M.

$\square$

Def: A commutative ring $\mathcal{O}$ is called a discrete valuation ring if $\mathcal{O}$ is a local principal ideal domain.

Ex: $\mathbb{Z}_{(p)}$ is a discrete valuation ring and $\widehat{(\mathbb{Z}_{(p)})} =: \widehat{\mathbb{Z}}_p$ is the ring of p-adic integers

the completion!

<u>Theorem 6</u> Let $\mathcal{O}$ be a discrete valuation ring and $\pi \in \mathcal{O}$, $\mathcal{J}(\mathcal{O}) = (\pi)$. Then
(i) $\forall \lambda \in \mathcal{O} \setminus \{0\}$, $\exists!$ max int. $\vartheta(\lambda)$, $\lambda \in \pi^{\vartheta(\lambda)} \cdot \mathcal{O}$.
(ii) $\forall \lambda, \mu$, $\vartheta(\lambda\mu) = \vartheta(\lambda) + \vartheta(\mu)$ and $\vartheta(\lambda+\mu) \geq \min\{\vartheta(\lambda), \vartheta(\mu)\}$
(iii) $\forall I \subseteq \mathcal{O}$ ideal, $I = \pi^n \mathcal{O}$ for some $n \geq 0$.

<u>Proof</u>: Take $\lambda \in \mathcal{O} \setminus \{0\}$.
$\mathcal{O} \supsetneq \pi\mathcal{O} \supsetneq \pi^2\mathcal{O} \supsetneq \cdots$ and $\bigcap_{k\geq 0} \pi^k \mathcal{O}$
so there exists a unique maximal $\vartheta(\lambda)$ s.th. $\lambda \in \pi^{\vartheta(\lambda)} \cdot \mathcal{O}$. In fact $\lambda = \pi^{\vartheta(\lambda)}\lambda'$ with $\lambda' \in \mathcal{O} \setminus \pi\mathcal{O} = \mathcal{O}^\times$. Thus $\lambda\mathcal{O} = \pi^{\vartheta(\lambda)}\mathcal{O}$ so every ideal is of the form $\pi^n \mathcal{O}$.
□

<u>Def</u>: An $\mathcal{O}$-module M is called <u>torsion free</u> if $\forall \lambda \in \mathcal{O}, m \in M$ $\lambda m = 0 \Rightarrow \lambda = 0$ or $m = 0$.

<u>Theorem 7</u> Let $\mathcal{O}$ be a discrete valuation ring and let M be finitely generated $\mathcal{O}$-module.
TFAE:
(i) M is free
(ii) M is projective
(iii) M is torsion-free.

<u>Proof</u>: (i) $\Leftrightarrow$ (ii) by Thm 3

$\mathcal{O}$ is an integral domain so (i) $\Rightarrow$ (iii)
(iii) $\Rightarrow$ (i) Let M be torsion-free
$M/\mathcal{J}(\mathcal{O})M$ is a k-vector space
Take $\{m_1, \ldots, m_n\} \subseteq M$ the preimages of a k-basis of $M/\mathcal{J}(\mathcal{O})M$.

Thus $\sum_{i=1}^{n} \mathcal{O} m_i + \mathcal{J}(\mathcal{O}) M = M$

and $\sum_{i=1}^{n} \mathcal{O} m_i = M$ by Nakayama's Lemma.

Hence $\{m_1, \dots, m_n\}$ is a generating system.

~~Take~~ $\sum \lambda_i m_i = 0$ a linear combination.
Given that the image in $M/\mathcal{J}(\mathcal{O})M$ is a linear combination of elements in a k-base we get that $\lambda_i \in \mathcal{J}(\mathcal{O}) = \pi \mathcal{O}$ $\forall i = 1, \dots, n$
But then $\lambda_i = \pi \lambda_i'$ and $\pi \cdot (\sum \lambda_i' m_i) = 0$.
Using that $\pi \neq 0$ and M is torsion free We get that $\sum \lambda_i' m_i = 0$. By the same argument as before $\lambda_i' \in \mathcal{J}(\mathcal{O}) = \pi \cdot \mathcal{O}$.
Hence $\lambda_i \in \pi^2 \mathcal{O}$, $\forall i$. By induction $\lambda_i \in \pi^k \mathcal{O}$, $\forall k$, $\forall i$ we get: $\lambda_i = 0$ $\forall i$
This gives that $\{m_1, \dots, m_n\}$ is lin. indep and hence a k-basis of M $\square$

<u>Corollary 8</u> Let $\mathcal{O}$ be a discrete valuation ring M a finitely generated free module. Then any submodule of M is free.
<u>Proof</u>: any submodule of M is torsion free $\square$

<u>Prop 9</u> Let $\mathcal{O}$ be a discrete valuation ring, let M be a free $\mathcal{O}$-module of finite rank and let N be a submodule of M. Then N is a direct summand of M iff $\mathcal{J}(\mathcal{O})N = \mathcal{J}(\mathcal{O})M \cap N$.

<u>Proof</u>: We always have $\mathcal{J}(\mathcal{O})N \subseteq \mathcal{J}(\mathcal{O})M \cap N$.
"$\Rightarrow$" Suppose N is a direct summand of M (<u>Notation</u>: $N \mid M$) Then $M = N \oplus N'$

Then $J(\mathcal{O})M = J(\mathcal{O})N \oplus J(\mathcal{O})N'$ and thus
$J(\mathcal{O})M \cap N = J(\mathcal{O})N$ (as $J(\mathcal{O})N' \subseteq N'$ and $N \cap N' = 0$)

"$\Leftarrow$" $J(\mathcal{O})M \cap N = J(\mathcal{O})N$.

We know that N is free. To prove that N is a summand of M it would be enough to show that M/N is free (then $M \twoheadrightarrow M/N$ splits)

We'll see that M/N is ~~torsion~~ free:

Take $\lambda \neq 0$ and $m \in M \setminus N$ ($\overline{m} \neq 0$ in M/N) such that $\overline{\lambda \cdot m} = 0$ ($\Leftrightarrow \lambda \cdot m \in N$)

- $\lambda \notin \mathcal{O}^\times$, otherwise $m \in N$. Thus $\lambda = \pi^n \lambda'$, $\lambda' \in \mathcal{O}^\times$
- $\pi^n \lambda' m \in J(\mathcal{O})M \cap N = J(\mathcal{O})N \Rightarrow \pi^n \lambda' m = \pi n$

$\Rightarrow \pi^{n-1} \lambda' m = n$ (as M is ~~torsion~~ free)

continuing by induction on n one gets $\lambda' m \in N$

$\Rightarrow m \in N \Rightarrow \Leftarrow$.

Hence M/N is ~~torsion~~ free $\square$

\!!!/ Remark:

- if χ is a char. of a group over a field, then χ takes values in the subring of alg integers of K
- if $K = Q(\mathcal{O})$ - quotient field, then $\mathcal{O}$ contains all algebraic integers of K (see next result)
  $\mathcal{O}$ discrete valuation ring
- hence χ is a map from G to $\mathcal{O}$
- stronger structural fact: $\forall$ fin. dim KG-module M there is an $\mathcal{O}G$-module U s.th. U is $\mathcal{O}$-free and $M \cong K \otimes_{\mathcal{O}} U$. If χ is a char of M then it is defined on $\mathcal{O}$. But moreover M is "defined" on $\mathcal{O}$.

<u>Thm 10</u> Let $\mathcal{O}$ be a principal ideal domain and let $K = Q(\mathcal{O})$ be the quot field. Then $\mathcal{O}$ is integrally closed; i.e. if $\alpha \in K$ is a root of a non-zero monic poly $f \in \mathcal{O}[X]$ then $\alpha \in \mathcal{O}$. In particular $\mathcal{O}$ contains the alg. integers of.

<u>Proof</u>. Let $f = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathcal{O}[X]$
Take $\alpha \in K$, $f(\alpha) = 0$. Write $\alpha = \frac{\beta}{\gamma}$, $\beta, \gamma \in \mathcal{O}$
$\mathcal{O}$ is a PID so $\mathcal{O}\beta + \mathcal{O}\gamma = \mathcal{O}\delta$, $\delta \in \mathcal{O}$.
in particular $\beta, \gamma \in \mathcal{O}\delta$. Dividing out δ one gets $\mathcal{O}\beta + \mathcal{O}\gamma = \mathcal{O}$ $(\Leftrightarrow a\beta + b\gamma = 1)$

<u>Aim</u>: prove $\mathcal{O}\beta^n \subseteq \mathcal{O}\gamma$ so that $\mathcal{O}\gamma = \mathcal{O}$ and $\gamma \in \mathcal{O}^\times$.

$$\beta^n + a_{n-1}\beta^{n-1}\gamma + \dots + a_0\gamma^n = 0 \Rightarrow \beta^n \in \mathcal{O}\gamma$$
$$\mathcal{O} = \mathcal{O}^n = (\mathcal{O}\beta + \mathcal{O}\gamma)^n \subseteq \mathcal{O}\beta^n + \mathcal{O}\gamma = \mathcal{O}\gamma$$
$$\Rightarrow \mathcal{O}\gamma = \mathcal{O} \Rightarrow \gamma \in \mathcal{O}^\times \text{ and } \alpha = \frac{\beta}{\gamma} \in \mathcal{O}. \quad \square$$

<u>Def</u> We say that a field <u>k is perfect</u> if $\begin{matrix} k \to k \\ \alpha \to \alpha^p \end{matrix}$ is surjective, where $p = \operatorname{char} k$.

<u>Thm 11</u> Let $\mathcal{O}$ be a complete, discrete valuation ring with $k = \mathcal{O}/\mathcal{J}(\mathcal{O})$ perfect, of prime char p.
The canonical group homomorphism $f: \mathcal{O}^\times \to k^\times$ splits:
$$\mathcal{O}^\times \simeq k^\times \times (1 + \mathcal{J}(\mathcal{O})).$$

<u>Proof</u> (idea)
$$\mathcal{O}^\times = \mathcal{O} - \mathcal{J}(\mathcal{O}) \text{ and thus } \ker f = (1 + \mathcal{J}(\mathcal{O}))$$

- first remark that $\delta - \gamma \in \pi^k\mathcal{O}$ implies that $\delta^p - \gamma^p \in \pi^{k+1}\mathcal{O}$ for $\delta, \gamma \in \mathcal{O}$. (exercise)
- let $\alpha \in k^\times$. Define $g(\alpha) := \lim_{e \geq 1} \beta_e$.

where β_e is defined as follows.

- $(\alpha_e)^{p^e} = \alpha$ (this determines α_e) – use k is perf
- β_e – preimage of α_e, rised to p^e.

Prove that:

- β_e is a Cauchy sequent
- g is a group homomorphism and a section of f. (exercises)
- show that g is unique

$\square$

Thm 12 (without proof)

Let k be a perfect field of positive char p. Then there is, up to isom, a unique complete discrete valuation ring $\mathcal{O}$ having char zero and residue field k such that $\mathcal{J}(\mathcal{O}) = p\mathcal{O}$.