Chapter 4. p-Modular Systems

R. Brauer started in the late 1920's a systematic investigation of group representations over fields of positive characteristic. In order to relate group representations over fields of positive characteristic to character theory in characteristic zero, Brauer worked with a triple of rings $(F, \mathcal{O}, k)$, called a *p-modular system*, and consisting of a complete discrete valuation ring $\mathcal{O}$ with a residue field $k := \mathcal{O}/J(\mathcal{O})$ of prime characteristic p and fraction field $F := \mathrm{Frac}(\mathcal{O})$ of characteristic zero. The present chapter contains a short introduction to these concepts. We will use p-modular systems and *Brauer 's reciprocity theorem* in the subsequent chapters to gain information about kG and its modules (which is/are extremely complicated) from the group algebra FG, which is semisimple and therefore much better understood, via the group algebra $\mathcal{O}G$. This explains why we considered arbitrary associative rings in the previous chapters rather than immediately focusing on fields of positive characteristic.

Notation. Throughout this chapter, unless otherwise specified, we let p be a prime number and G denote a finite group. For each $K \in \{F, \mathcal{O}, k\}$ all KG-modules are assumed to be **finitely generated and free** as K-modules .

References:

[CR90] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I.* John Wiley & Sons, Inc., New York, 1990.

[Lin18] M. Linckelmann. *The block theory of finite group algebras. Vol. I.* Vol. 91. London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 2018.

[NT89] H. Nagao and Y. Tsushima. *Representations of finite groups*. Academic Press, Inc., Boston, MA, 1989.

[Ser68] Jean-Pierre Serre. *Corps locaux*. Deuxième édition, Publications de l'Université de Nancago, No. VIII. Hermann, Paris, 1968.

[Thé95] J. Thévenaz. *G-algebras and modular representation theory*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1995.

[Web16] P. Webb. *A course in finite group representation theory*. Vol. 161. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2016.

13 Complete discrete valuation rings

In this section we review some number-theoretic results without formal proofs. I refer students to their number theory lectures for details, or to [Ser68; Lin18; Thé95]. Important for the sequel is to keep definitions and examples in mind.

To begin with, recall from Chapter 1, §5, that a commutative ring $\mathcal{O}$ is local iff $\mathcal{O}\setminus\mathcal{O}^\times = J(\mathcal{O})$, i.e. $J(\mathcal{O})$ is the unique maximal ideal of $\mathcal{O}$. Moreover, by the commutativity assumption this happens if and only if $\mathcal{O}/J(\mathcal{O})$ is a field. We write $k := \mathcal{O}/J(\mathcal{O})$ and call this field **the residue field of (the local ring)** $\mathcal{O}$. To ease up notation, we will often write $\mathfrak{p} := J(\mathcal{O})$. This is because our aim is a situation in which the residue field is a field of positive characteristic p.

Definition 13.1 (***Reduction modulo*** $\mathfrak{p}$)

Let $\mathcal{O}$ be a local commutative ring with unique maximal ideal $\mathfrak{p} := J(\mathcal{O})$ and residue field $k := \mathcal{O}/\mathfrak{p}$. Let M, N be finitely generated $\mathcal{O}$-modules, and let $f : M \longrightarrow N$ be an $\mathcal{O}$-linear map.

(a) The k-module $\overline{M} := M/\mathfrak{p}M \cong k \otimes_{\mathcal{O}} M$ is called the **reduction modulo** $\mathfrak{p}$ of M.

(b) The induced k-linear map $\overline{f} : \overline{M} \longrightarrow \overline{N}$, $m+\mathfrak{p}M \mapsto f(m)+\mathfrak{p}N$ is called the **reduction modulo** $\mathfrak{p}$ of f.

Exercise 13.2

Let $\mathcal{O}$ be a local commutative ring with unique maximal ideal $\mathfrak{p} := J(\mathcal{O})$ and residue field $k := \mathcal{O}/J(\mathcal{O})$.

(a) Let M, N be finitely generated free $\mathcal{O}$-modules.

  (i) Let $f : M \longrightarrow N$ be an $\mathcal{O}$-linear map and $\overline{f} : \overline{M} \longrightarrow \overline{N}$ its reduction modulo $\mathfrak{p}$. Prove that if $\overline{f}$ is surjective (resp. an isomorphism), then f is surjective (resp. an isomorphism).

  (ii) Prove that if elements $x_1, \dots, x_n \in M$ ($n \in \mathbb{Z}_{\geqslant 1}$) are such that their images $\overline{x}_1, \dots \overline{x}_2 \in \overline{M}$ form a k-basis of $\overline{M}$, then $\{x_1, \dots, x_n\}$ is an $\mathcal{O}$-basis of M.
  In particular, $\dim_k(\overline{M}) = \mathrm{rk}_{\mathcal{O}}(M)$.

(b) Deduce that any direct summand of a finitely generated free $\mathcal{O}$-module is free.

(c) Prove that if M is a finitely generated $\mathcal{O}$-module, then the following conditions are equivalent:

  (i) M is projective;

  (ii) M is free.

  Moreover, if $\mathcal{O}$ is also a PID, then (i) and (ii) are also equivalent to:

  (iii) M is torsion-free.

[Hint: Use Nakayama's Lemma.]

Definition 13.3

A commutative ring $\mathcal{O}$ is called a **discrete valuation ring** if $\mathcal{O}$ is a local principal ideal domain such that $J(\mathcal{O}) \neq 0$.

Example 7

Let p be a prime number. We have already seen in Example 1(b) that the ring $\mathbb{Z}_{(p)} := \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$ is commutative local with unique maximal ideal

$$J(\mathbb{Z}_{(p)}) = \{\frac{a}{b} \in \mathbb{Z}_{(p)} \mid p \mid a\} = p\mathbb{Z}_{(p)}\,.$$

It follows easily that $\mathbb{Z}_{(p)}$ is a PID (every non-zero ideal in $\mathbb{Z}_{(p)}$ is of the form $p^n\mathbb{Z}_{(p)}$ for some integer $n \in \mathbb{Z}_{\geqslant 0}$), hence a *discrete valuation ring*.

In fact this example is a special case of a more general construction for discrete valuation rings, which consists in taking $\mathcal{O} := R_\mathfrak{p}$, where R is the ring of algebraic integers of an algebraic number field and $R_\mathfrak{p}$ is the localisation of R at a non-zero prime ideal $\mathfrak{p}$ in R.

Remark 13.4

There is in fact a link between Definition 13.3 and the theory of valuations explaining the terminology *discrete valuation ring*, provided by the following result. (Not difficult to prove!)

Theorem 13.5

Let $\mathcal{O}$ be a discrete valuation ring and let $\pi \in \mathcal{O}$ such that $J(\mathcal{O}) = \pi\mathcal{O}$. Then:

(a) For every $a \in \mathcal{O}\backslash\{0\}$ there is a unique maximal (non-negative) integer $v(a)$ such that $a \in \pi^{v(a)}\mathcal{O}$.

(b) For any $a, b \in \mathcal{O}\backslash\{0\}$ we have $v(ab) = v(a) + v(b)$ and $v(a + b) \geqslant \min\{v(a), v(b)\}$.

(c) Every non-zero ideal in $\mathcal{O}$ is of the form $\pi^n\mathcal{O}$ for some unique integer $n \in \mathbb{Z}_{\geqslant 0}$.

The map $v : \mathcal{O}\backslash\{0\} \longrightarrow \mathbb{Z}$ defined in this way is called the **valuation** of the discrete valuation ring $\mathcal{O}$.

One can use valuations to give an alternative definition of *valuation rings*. Suppose that F is a field and that $v : F^\times \longrightarrow \mathbb{Z}$ is a surjective map satisfying

· $v(ab) = v(a) + v(b)$ (so v is a group homomorphism $\Rightarrow v(1) = 0$ and $v(a^{-1}) = -v(a)$), and

· $v(a + b) \geqslant \min\{v(a), v(b)\}$,

for all $a, b \in F^\times$, and we set for notational convenience $v(0) = \infty$. Then, the set

$$\mathcal{O} := \{a \in F \mid v(a) \geqslant 0\}$$

is a discrete valuation ring, and $F = \mathrm{Frac}(\mathcal{O})$ is the fraction field of $\mathcal{O}$. Clearly, the unique maximal ideal in $\mathcal{O}$ is

$$J(\mathcal{O}) = \{a \in F \mid v(a) \geqslant 1\} = \mathcal{O}\backslash\mathcal{O}^\times .$$

Taking for π any element in $\mathcal{O}$ such that $v(\pi) = 1$, one easily checks that $\mathcal{O}$ has the properties stated in the theorem above.

A valuation induces a metric, and hence a topology. For the purpose of representation theory of finite groups, we will need to focus on the situation in which this topology is complete. This can be expressed algebraically as follows.

Definition 13.6 (*Complete discrete valuation ring*)

Let $\mathcal{O}$ be a discrete valuation ring with unique maximal ideal $\mathfrak{p} := J(\mathcal{O})$.

(a) A sequence $(a_m)_{m\geqslant 1}$ of elements of $\mathcal{O}$ is called a **Cauchy sequence** if for every integer $b \geqslant 1$, there exists an integer $N \geqslant 1$ such that $a_m - a_n \in \mathfrak{p}^b$ for all $m, n \geqslant N$.

(b) The ring $\mathcal{O}$ is called **complete (with respect to the $\mathfrak{p}$-adic topolog)** if for every Cauchy sequence $(a_m)_{m\geqslant 1} \subseteq \mathcal{O}$ there is $a \in \mathcal{O}$ such that for any integer $b \geqslant 1$ there exists an integer $N \geqslant 1$ such that $a - a_m \in \mathfrak{p}^b$ for all $m \geqslant N$. (In this case, a is a **limit** of the Cauchy sequence $(a_m)_{m\geqslant 1}$.)

Remark 13.7

The previous definition can be generalised to a finitely generated $\mathcal{O}$-algebra A. Moreover, one can prove that A is complete in the $J(A)$-adic topology if $\mathcal{O}$ is complete in the $J(\mathcal{O})$-adic topology.

Example 8

Let p be a prime number. The discrete valuation ring $\mathbb{Z}_{(p)}$ is not complete. However, its completion, the ring of p-adic integers, that is,

$$\hat{\mathbb{Z}}_{(p)} = \mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i \,\middle|\, a_i \in \{0, \dots, p-1\} \,\forall\, i \geqslant 0 \right\} ,$$

is a complete discrete valuation ring. Its field of fractions is $\mathrm{Frac}(\mathbb{Z}_p) = \mathbb{Q}_p$ (i.e. the field of p-adic integers), $J(\mathbb{Z}_p) = p\mathbb{Z}_p$ and the residue field is $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

Finally we mention without proof a very useful consequence of Hensel's Lemma.

Corollary 13.8

Let $\mathcal{O}$ be a complete discrete valuation ring with unique maximal ideal $\mathfrak{p} := J(\mathcal{O})$ and residue field $k := \mathcal{O}/\mathfrak{p}$ of prime characteristic p, and let $m \in \mathbb{Z}_{\geqslant 1}$ be coprime to p. Then, for any m-th root of unity $\zeta \in k$, there exists a unique m-th root of unity $\mu \in \mathcal{O}$ such that $\overline{\mu} = \zeta$.

14 Splitting p-modular systems

In order to relate group representations over a field of positive characteristic to character theory in character zero, Brauer worked with *p-modular systems*.

Definition 14.1 (*p-modular systems*)

Let p be a prime number.

(a) A triple of rings $(F, \mathcal{O}, k)$ is called a **p-modular system** if:

(1) $\mathcal{O}$ is a complete discrete valuation ring of characteristic zero,

(2) $F = \mathrm{Frac}(\mathcal{O})$ is the field of fractions of $\mathcal{O}$ (also of characteristic zero), and

(3) $k = \mathcal{O}/J(\mathcal{O})$ is the residue field of $\mathcal{O}$ and has characteristic p.

(b) Given a finite group G, a p-modular system $(F, \mathcal{O}, k)$ is called a **splitting p-modular system for** G, if both F and k are splitting fields for G.

It is often helpful to visualise p-modular systems and the condition on the characteristic of the rings involved through the following commutative diagram of rings and ring homomorphisms

$$\begin{tikzcd} \mathbb{Q} \arrow[d, hook] & \mathbb{Z} \arrow[l, hook'] \arrow[r, two heads] \arrow[d, hook] & \mathbb{F}_p \arrow[d, hook] \\ F & \mathcal{O} \arrow[l, hook'] \arrow[r, two heads] & k \end{tikzcd}$$

where the hook arrows are the canonical inclusions and the two-head arrows the quotient morphisms. Clearly, these morphisms also extend naturally to ring homomorphisms

$$FG \hookleftarrow \mathcal{O}G \twoheadrightarrow kG$$

between the corresponding group algebras (each mapping an element $g \in G$ to itself).

Example 9

One usually works with a splitting p-modular system for all subgroups of G, because it allows us to avoid problems with field extensions. By a theorem of Brauer on splitting fields such a p-modular system can always be obtained by adjoining a primitive m-th root of unity to $\mathbb{Q}_p$, where m is the exponent of G. (Notice that this extension is unique.) So we may as well assume that our situation is as given in the following commutative diagram:

$$\begin{tikzcd} \mathbb{Q}_p \arrow[d, hook] & \mathbb{Z}_p \arrow[l, hook'] \arrow[r, two heads] \arrow[d, hook] & \mathbb{F}_p \arrow[d, hook] \\ F & \mathcal{O} \arrow[l, hook'] \arrow[r, two heads] & k \end{tikzcd}$$

More generally, we have the following result, which we mention without proof. The proof can be found in [CR90, §17A].

Theorem 14.2

Let $(F, \mathcal{O}, k)$ be a p-modular system. Let G be a finite group of exponent $\exp(G) =: m$. Then the following assertions hold.

(a) The field F contains all m-th roots of unity if and only if F contains the cyclotomic field of m-th roots of unity.

(b) If F contains all m-th roots of unity, then so does k, and F and k are splitting fields for G and all its subgroups.

Remark 14.3

If $(F, \mathcal{O}, k)$ is a p-modular system, then it is not possible to have F and k algebraically closed, while assuming $\mathcal{O}$ is complete. (Depending on your knowledge on valuation rings, you can try to prove this as an exercise!)

Let us now investigate changes of the coefficients given in the setting of a p-modular system for group algebras involved.

Definition 14.4

Let $\mathcal{O}$ be a commutative local ring. A finitely generated $\mathcal{O}G$-module L is called an **$\mathcal{O}G$-lattice** if it is free (= projective) as an $\mathcal{O}$-module.

Remark 14.5 (*Changes of the coefficients*)

Let $(F, \mathcal{O}, k)$ be a p-modular system and write $\mathfrak{p} := J(\mathcal{O})$. If L is an $\mathcal{O}G$-module, then:

- setting $L^F := F \otimes_{\mathcal{O}} L$ defines an FG-module, and
- reduction modulo $\mathfrak{p}$ of L, that is $\overline{L} := L/\mathfrak{p}L \cong k \otimes_{\mathcal{O}} L$ defines a kG-module.

We note that, when seen as an $\mathcal{O}$-module, an $\mathcal{O}G$-module L may have torsion, which is lost on passage to F. In order to avoid this issue, we usually only work with $\mathcal{O}G$-lattices. In this way, we obtain functors

$$FG\text{-}\mathbf{mod} \longleftarrow \mathcal{O}G\text{-}\mathbf{lat} \longrightarrow kG\text{-}\mathbf{mod}$$

between the corresponding categories of finitely generated $\mathcal{O}G$-lattices and finitely generated FG-, kG-modules.

A natural question to ask is: which FG-modules, respectively kG-modules, come from $\mathcal{O}G$-lattices? In the case of FG-modules we have the following answer.

Proposition-Definition 14.6

Let $\mathcal{O}$ be a complete discrete valuation ring and let $F := \mathrm{Frac}(\mathcal{O})$ be the fraction field of $\mathcal{O}$. Then, for any finitely generated FG-module V there exists an $\mathcal{O}G$-lattice L which has an $\mathcal{O}$-basis which is also an F-basis. In this situation $V \cong L^F$ and we call L an **$\mathcal{O}$-form** of V.

Proof: Choose an F-basis $\{v_1, \dots, v_n\}$ of V and set $L := \mathcal{O}Gv_1 + \dots + \mathcal{O}Gv_n \subseteq V$.
Exercise: verify that L is as required. ■

For kG-modules the situation is much more complicated. This is why, we introduce the following definition.

Definition 14.7 (*Liftable kG-module*)

Let $\mathcal{O}$ be a commutative local ring with unique maximal ideal $\mathfrak{p} := J(\mathcal{O})$ and residue field $k := \mathcal{O}/\mathfrak{p}$. A kG-module M is called **liftable** if there exists an $\mathcal{O}G$-lattice $\widehat{M}$ whose reduction modulo $\mathfrak{p}$ is isomorphic to M, that is,

$$\widehat{M}/\mathfrak{p}\widehat{M} \cong M\,.$$

(Alternatively, it is also said that M is **liftable to an $\mathcal{O}G$-lattice**, or **liftable to $\mathcal{O}$**, or **liftable to characteristic zero**.)

Even though every $\mathcal{O}G$-lattice can be reduced modulo $\mathfrak{p}$ to produce a kG-module, not every kG-module is liftable to an $\mathcal{O}G$-lattice. Being liftable for a kG-module is a rather rare property. However, the next chapters will bring us some answers towards classes of kG-modules made up of liftable modules.