An Introduction to Non-Commutative Rings,Representations of Groups and Local Fields

Student:
Ayush Kumar Tewari
Roll No. : 1211011
Summer Project Report
National Institute of Science Education and Research, Bhubaneswar

Guide:
Dr. B Sury
Professor ,STAT-MATH Unit
Indian Statistical Institute, Bangalore

PART - 1 - NON COMMUTATIVE RINGS AND REPRESENTATION OF GROUPS

Contents

Preface

The theory of Non Commutative Ring theory has gone forward with the most transitional phase in the latter part of the 20th century , initially starting with a very natural Wedderburn-Artin Theory, which also has natural occurrences in the study of Lie Groups and Algebras,leading into Jacobson Radical Theory and then moving onto group rings and representations of groups and algebras.The end results of these theories provide a very innovative outlook to even problems related to different aspects of mathematics like Representation theory ,Central Simple Algebras , Group-cohomology .

In this report , I would like to bring in new insight into the theory of non commutative rings , by going through the pre established theories , and ultimately looking at the results , such that we have a better view of the applicative aspects of the theory in the field of representation theory .
The latter part of this report deals with the introduction to local fields , which involves the study of fields which are equipped with a innate topology induced by the valuation inherited from the base ring , which in order gives them very nice structure , namely completeness . In the last part I have tried to talk about the basics regarding local fields and some introductory results in this field which would help to develop a better insight into the detailed version of the theory.

0.1 Wedderburn-Artin Theorem and Semisimplicity

0.1.1 Semi Simplicity

Definition. *Let R be a ring and M be a (left) R-module.*

- *M is called a simple (or irreducible) R-module if $M \neq 0$ and M has no other R-sub-modules than (0) and R.*
- *M is called semi-simple(or completely reducible) R-module if every R-sub-module of M is an R-module direct summand of M.*

Lemma. *Any non-zero semisimple R-module M contains a simple sub-module.*

Proof. Let m a fixed non-zero element of M . It suffices to treat the case when M = m. By Zorn's Lemma , there exists a sub-module N of M maximal with respect to the property that $m \notin N$. Take a (necessarily nonzero) submodule N' such that $M = N \oplus N'$. We finish by showing that N' is simple . Indeed if N" is a nonzero submodule of N', then $N \oplus N$" contains m (by the maximality of N), and so $N \oplus N$" $= M$, which clearly implies that N" = N', as desired .

Theorem 1. *For an R-module $M = {}_RM$, the following three properties are equivalent :-*

1. *M is semisimple.*
2. *M is the direct sum of a family of simple submodules .*
3. *M is the sum of a family of simple submodules*

Proof. $1 \longrightarrow 3$
Let M_1 be the sum of all simple submodules in M and write $M = M_1 \oplus M_2$ where M_2 is a suitable R-submodule. If $M_2 \neq 0$, the Lemma implies that M_2 contains a simple R-submodule .But the latter must lie in M_1, a contradiction.Thus, $M_2 = (0)$; i.e., $M_1 = M_2$.
$3 \longrightarrow 1$
Write M = $\sum_{i \in I} M_i$, where M_i's are simple submodules of M . Let $N \subseteq M$ be a given submodule . To show that N is a direct summand of ${}_RM$, consider subsets J $\subseteq$ I with the following properties :

- $\sum_{j \in J} M_j$ is a direct sum.
- $N \cap \sum_{j \in J} M_j = (0)$

The Zorn's Lemma applies to the family of all such J's with respect to ordinary inclusion.(This is a non empty family as it contains the empty set.)Thus,we can pick a J to be maximal.For this J,let

$$M' := N + \sum_{j \in j} M_j = N \oplus \bigoplus_{j \in J} M_j \tag{1}$$

We finish by showing that $M' = M$ (for then N is a direct summand of ${}_RM$.)For this, it suffices to show that $M' \supset M_i \ \forall$ i $\in I$ .But if some $M_i \subseteq M'$,the simplicity of M_i implies that $M' \cap M_i = (0)$.From this we have

$$M' + M_i = N \oplus \bigoplus_{j \in J} M_j \oplus M_i, \tag{2}$$

in contradiction to the maximality of J.
$3 \longrightarrow 2$
follows from the argument above applied to $N = (0)$.
$2 \longrightarrow 3$
is a tautology. QED
* The semi-simplicity defined here is essentially the notion which is given by Wedderburn's theory , we would be later stating the semi-simplicity defined by the Jacobson's radical theory and will be showing the equivalence of both in the latter part of this text.

Theorem 2. *Let D be a division ring, and let $R = \mathbb{M}_n(D)$. Then*

1. *R is simple,left semi-simple,left artinian and left noetherian.*
2. *R has (up to isomorphisms) a unique left simple module V.R acts faithfully on V, and ${}_RR \cong n.V$ as R-modules.*
3. *The endomorphism ring $End({}_RV)$,viewed as a ring of right operators on V, is isomorphic to D.*

Proof. Since D is a simple ring, the simplicity of R follows because we know that the ideals of $\mathbb{M}_n(D)$ look like $\mathbb{M}_n(I)$, where I is an ideal of R . We may view $R = \mathbb{M}_n(D)$ as a left D-vector space ,and, as such R has finite D-dimension n^2.Since the left ideals of R are subspaces of R it is clear that they must satisfy the DCC as well as ACC .
Let V be the n-tuple column space D^n,viewed as a right D-vector space . The ring R = $\mathbb{M}_n(D)$ acts on the left of V by matrix multiplication,so we can view V as a left R-module. In fact R may be identified with $End(V_D)$ bu using the usual matrix representation of linear transformations . This shows that ${}_RV$ is a faithful R-module and this implies it is a simple R-module .
Now consider the direct sum decomposition

$$R = \mathbb{U}_1 \oplus \mathbb{U}_2 ..... \oplus \mathbb{U}_n$$

where each $\mathbb{U}_i$ is in the left ideal of R consisting of matrices all of whose columns other than the i^{th} are equal to zero .As a left R-module,$\mathbb{U}_i$ is clearly isomorphic to ${}_RV$, so ${}_RR \cong n.V$ is semi-simple. This shows that the ring R is left semi-simple . To show the uniqueness of V , let V' be another simple left R-module.Since $V' \cong R/m$ for some maximal left ideal , $m \subset R$. So V' is a composition factor of ${}_RR$.Therefore, by the Jordan Holder's Theorem, it follows that $V' \cong V$. Let us compute E:=End(${}_RV$).We have a natural ring homomorphism

$$\delta : D \to E$$

$$v.\delta(d) = v.d \ (\ v \in V, d \in D)$$

The proof will be complete if we can show that δ is an isomorphism .The injectivity of δ is clear since D acts faithfully on V_D.To prove the surjectivity of δ ,consider $f \in E$. Writing

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{pmatrix} .f = \begin{pmatrix} d \\ * \\ \vdots \\ \vdots \\ \vdots \\ * \end{pmatrix} (d \in D) \tag{3}$$

$$\begin{pmatrix} a_1 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ a_n \end{pmatrix} f = \left(\begin{pmatrix} a_1 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ a_n & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{pmatrix} \right) f = \begin{pmatrix} a_1 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ a_n & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} d \\ * \\ \vdots \\ \vdots \\ \vdots \\ * \end{pmatrix}$$

$$= \begin{pmatrix} a_1 d \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ a_n d \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ a_n \end{pmatrix} \delta(d)$$

(4)

Hence f = $\delta(d)$ QED.

Proposition. *Let $R_1, \ldots, R_n$ be left semisimple rings. Then their direct product $R = R_1 \times \ldots \times R_r$ is also a left semisimple ring.*

Proof. Let $R = \mathbb{U}_{i1} \oplus \ldots \oplus \mathbb{U}_{im_i}$, where each $\mathbb{U}_{ij}$ is a minimal left ideal of R_i.Viewing R as an ideal in R, $\mathbb{U}_{ij}$ is also a minimal left ideal of R.From

$$_RR = R_1 \oplus \ldots \oplus R_r = \bigoplus_{j \in J} \mathbb{U}_{ij}$$

We conclude that R is semisimple . QED

0.1.2 Wedderburn-Artin-Theorem

Theorem (Wedderburn-Artin Theorem)**.** *Let R be any left semisimple ring . Then $R \cong \mathbb{M}_{n_1}(D_1) \times \ldots \times \mathbb{M}_{n_r}(D_R)$ for suitable rings $D_1, D_2, ...D_r$ and positive integers $n_1, n_2, ..., n_r$ .The number r is uniquely determined , as are the pairs $(n_1, D_1), ..., (n_r, D_r)$ (up to permutations). There are exactly r mutually non-isomorphic left simple modules over R.*

Before proving the theorem we would prove the very useful Lemma by Schur.

Lemma (Schur's Lemma)**.** *Let R be any ring and ${}_RV$ be any simple left R-module.Then $End({}_RV)$ is a division ring.*

Proof. Let $0 \neq f \in End({}_RV)$.Then $im(f) \neq 0$ and $ker(f) \neq V$.Since im(f) and ker(f) are both submodules of V, it follows that $im(f) = V$ and $ker(f) = 0$,i.e.,f is invertible in $End({}_RV)$. Therefore $End({}_RV)$ is a division ring . QED

Proof of Theorem Let R be any left semisimple ring .First we decompose ${}_RR$ into a finite direct sum of minimal left ideals.Grouping these according to their isomorphism types as left R-modules , we can write

$$ {}_RR \cong n_1V_1 \oplus \ldots \oplus n_rV_r, \tag{5}$$

where $V_1, \ldots, V_r$ are mutually non-isomorphic simple left R-modules.If V is any simple left R-module , we know that $V \cong R/m$, where m is a maximal ideal , so in any case if V is a simple R-module it is isomorphic to a quotient of ${}_RR$ and hence by Jordan-Holder's Theorem, V is isomorphic to some V_i.Therefore $\{V_1, \ldots, V_r$ is a full set of mutually isomorphic left simple R-modules . Let us now compute the R-endomorphism rings of the modules in (5),For ${}_RR$, the R-endomorphisms are given by right multiplication by elements of R, so

Claim (Claim -1)**.** $End({}_RR) \cong R$

Proof. Define a mapping $\phi : R \to End_R(R)$

$$\phi(\mathrm{r})(\mathrm{a}) = \mathrm{ar} \text{ for any a} \in \mathrm{R} \text{ , (r} \in \mathrm{R} \text{)and since}$$
$$\phi(r)(\mathrm{ab}) = (\mathrm{ab})\mathrm{r} = \mathrm{a}(\mathrm{br}) = \mathrm{a}(\phi(r)(\mathrm{b}))$$
$$\implies \phi \in End_R(R).\text{Similarly}$$
$$\phi(\mathrm{r})(\mathrm{a+b}) = (\mathrm{a+b})\mathrm{r} = \mathrm{ar} + \mathrm{br} = \phi(\mathrm{r})(\mathrm{a}) + \phi(\mathrm{r})(\mathrm{b})$$
$$\phi(\mathrm{r})(\mathrm{ab}) = \phi(\mathrm{r})(\mathrm{a})\phi(\mathrm{r})(\mathrm{b})$$
$\implies \phi$ is a ring homomorphism. and if $\phi(\mathrm{r}) = 0$, then $0 = \phi(\mathrm{r})(1) = \mathrm{r}$, so ϕ is one-one. and if if $\delta \in End_R(R)$, then for r : $= \delta(1)$,we have

$\phi(\mathrm{r})(\mathrm{a}) = \mathrm{ar} = \mathrm{a}\delta(1) = \delta(\mathrm{a})$ and since this is true $\forall$ a $\in$ R , $\therefore \phi(\mathrm{r}) = \delta$.
$\therefore \phi$ is also onto .
Hence , the claim. QED

Now returning back to the proof of the theorem , to compute $End(n_1V_1 \oplus \ldots \oplus n_rV_r)$, let $D_i = End(V_i)$. By Schur's Lemma each D_i is a a division ring , and

Claim (Claim -2)**.** $End(n_iV_i) \cong \mathbb{M}_{n_i}(D_i)$

Proof. Let $\epsilon_j : V_i \to n_iV_i$ be the j^th inclusion, and $\pi_i : n_iV_i \to V_i$ be the i^th projection. For any endomorphism F : $n_iV_i \to n_iV_i$, let f_{ij}be the composition of $\pi_iF\epsilon_j \in D_i$.Define a map

$$\alpha : End_R(n_iV_i) \to \mathbb{M}_n(D_i)$$

by $\alpha(F) = f_{ij}$.Its trivial to check that α is an isomorphism of rings .

Hence the claim. QED

Since there is no non zero homomorphism from V_i to V_j for $i \neq j$, we have

$$End(n_1V_1 \oplus \ldots \oplus n_rV_r) \cong End(n_1V_1) \times \ldots \times End(n_rV_r)$$

$$\cong \mathbb{M}_{n_i}(D_i) \times \ldots \times \mathbb{M}_{n_r}(D_r)(6)$$

thus we get a ring isomorphism

$$\mathrm{R} \cong \mathbb{M}_{n_i}(D_i) \times \ldots \times \mathbb{M}_{n_r}(D_r).$$

0.2 Jacobson-radical-theory

The Wedderburn's theory of semi-simplicity can be extended to rings satisfying the descending chain condition , i.e , Artininan rings . For a Artin ring , the sum of two nilpotent ideals is nilpotent , so R has a largest nilpotent ideal rad R , called the *Wedderburn radical* of R.
On the other hand , the *Jacobson radical* of a ring R , denoted by rad R, is defined to be the intersection of all maximal left ideals.

Lemma. *For $y \in R$, the following statements are equivalent :*

1. *$y \in R$*
2. *1 - xy is left invertible for any $x \in R$.*
3. *$yM = 0$ for any simple left R-module M.*

Proof. $1 \implies 2$
Assume $y \in radR$. If, for some x, $1-xy$ is not left invertible, then $R.(1-xy) \subset$ R is contained in a maximal left ideal m of R.But $1-xy \in m$ and$y \in m$ implies that $1 \in m$, a contradiction.
$2 \implies 3$
Assume $ym \neq 0$ for some $m \in M$.Then we must have $R.ym = M$.In particular,$m = x.ym$ for some $x \in R$,so $(1-xy)m = 0$.Using 2, we get $m = 0$, a contradiction.
$3 \implies 1$
For any maximal ideal m of R ,R/m is a simple left R-module ,so by 3 $y.R/m = 0$ which implies that ym .By definition, we have $y \in radR$. QED
For any left R-module M , the annihilator of M is defined to be
$annM := \{r \in R : rM = 0\}$ This is by definition an ideal of R . If we consider a cyclic module M, then $M \cong R/U$, where U is an ideal of R.Then,
ann M = $\{r \in R : r.R/U = 0\} = \{r \in R : rR \subset U\}$
i.e.,ann M is the largest ideal contained in U .This gives another classification of the Jacobson radical

Corollary 0.1. *rad $R = \cap$ ann M,where M ranges over all the simple left R-Modules.In particular,rad R is an ideal of R.*

Definition. *A ring R is called J-semisimple if rad R = 0.*

Lemma. *A one-sided ideal $U \subset R$ is said to be **nil** if U consists of nilpotent elements : U is said to be **nilpotent** if $U^n = 0$ for some natural number n .*

* nilpotent $\implies$ nil , but the converse is not true

Theorem 3. *Let be a one sided nil ideal in a right Noetherian ring R. Then A is nilpotent.*

Proof. Since R is right Noetherian it has a maximal nilpotent ideal N.Our aim is to show that $A \in N$.If not by passing to $\bar{R} = R/N$ we reach the following situation ; $\bar{R}$ is a right Noetherian ring which has no non-zero nilpotent ideals and $\bar{A} \neq 0$ is a nil one sided ideal of $\bar{R}$.We wish to that is impossible.In other words,we may assume without loss of generality,that R has no nilpotent ideals but has a nil one sided ideal A $\neq 0$.
If a $\neq 0 \in$ A ,then U = Ra is a nil left ideal of R, for if A is a left ideal of R , then since U $\subset$ A it,too,would be nil.If,on the other hand, A is a right ideal and u = za $\in$ U, then $u^n = x(ax)^{n-1}a$ is 0 for large value of n , since ax $\in$ A. If u $\in$ U, let r(u) = $\{x \in R | ux = 0\}$; r(u)is a non-zero right ideal of R.R being Noetherian, there is an $u_o \neq 0$ in U with $r(u_o)$ maximal.For any $x \in R$ clearly $r(xu_o) \supset r(u_o)$ hence,if $xu_o \neq 0$ since it is in U , we get $r(xu_o) = r(u_o)$ from the maximality of $r(u_o)$.Let y $\in$ R ; then $(yu_o)^k = 0$ and $yu_0^{k-1} \neq 0$ for some k.Because (yu_o^{k-1}) is of form xu_o we have a $r(yu_o)^{k-1} = r(u_o)$.But yu_o is in $r((yu_o)^{k-1})$ so is in $r(u_o)$;that is $u_o(yu_o) = 0$ for all y $\in$ R.This says that u_oR is nilpotent right ideal of R, hence is (0).But then $\{t \in R | tR = 0\}$ is a non-zero nilpotent right ideal (containing u_o).With this contradiction, the theorem is proved. QED

Proposition. *Let $x \in radR$,where R is a k-algebra.Then x is algebraic over k iff x is nilpotent .*

Proof. Firstly if x is nilpotent $\implies$ $x^n = 0$, therefore x is a root of the polynomial $f(x) = x^n$, hence is algebraic.Conversely ,let x $\in$ rad R be algebraic over k.Write down a polynomial equation for x in ascending degrees say

$$x^r + a_1x^{r-1} + \ldots + a_nx^{r+n} = 0 \text{ where } a_i \in k.\text{Since}$$

$$1 + a_1x + \ldots + a_nx^n \in 1 + radR \subseteq U(R),$$

it follows that $x^r = 0$ so we must have $r \geq 1$ and x is nilpotent. QED
A k-algebra is said to be an *algebraic algebra* if every element $x \in R$ is algebraic over k.The proposition then implies the following corollary:-

Corollary 0.2. *Let R be an algebraic algebra over k. Then rad R is the largest nil ideal of R .*

Theorem 4 (Amitsur)**.** *Suppose that $dim_kR < |k|$ (as cardinal numbers), where R is a k-algebra .Then rad R is the largest nil ideal of R .*

Proof. It suffices to show that rad R is nil.First suppose k is a finite field.The hypothesis implies that R is a finite ring .In particular R is left artinian and noetherian,so rad R is,in fact,nilpotent.In the following,we may therefore assume that k is infinite.To show that rad R is nil,it suffices to show that every r $\in R$is algebraic over k .For any a $\in$ k =k $\{0\}$, $a - r = a(1 - a^{-1}r) \in$ U(R).Since $dim_kR < k = |k| = |k^*|$,the elements $\{(a-r)^{-1} : a \in k^*\}$ cannot be k-linearly

independent.Therefore,there exist distinct elements $a_1 \ldots, a_n \in k^*$such that there is a dependence relation

$$\sum_{i=1}^{n} b_i(a_i - r)^{-1} = 0$$

where $b_i \in$ k are not all zero.Clearing denominators, we have

$$\sum_{i=1}^{n} b_i(a_1 - r) \ldots \overbrace{(a_i - r)} \ldots (a_n - r) = 0$$

where,as usual,the overhead braces means omission of a factor.Therefore ,r is root of the k-th polynomial

$$f(x) = \sum b_i(a_i - x) \ldots \overbrace{(a_i - x)} \ldots (a_n - x)$$

Since $f(a_i) = b_i \prod_{j \neq i}(a_j - a_i)$ is non-zero at least for some i ,f is not the zero polynomial.Therefore,r is algebraic over k, as claimed.

Lemma (Nakayama's Lemma)**.** *For any left ideal $J \subseteq R$, the following statements are equivalent:*

1. *$J \subseteq R$*
2. *For any finitely generated left R-module M, $J.M = M$ implies that $M = 0$.*
3. *For any left R-modules $N \subseteq M$ such that M/N is finitely generated, $N + J.M = M$,implies that $N = M$.*

Proof. $1 \implies 2$
Assume M $\neq$ 0.Then,among all submodules $\subset$ M,there is a maximal one,say M'.(This M' exists by Zorn's Lemma,in view of the finite generation of M.)Then M/M' is simple, so J.(M/M') = 0; i.e.,J.M $\subseteq$ M'.In particular, J.M $\neq$ M.
$2 \implies 3$
when we consider the quotient module M/N , applying (2) to this finitely generated module gives J.(M/N) = M/N, so let N' $\subset$ M/N , then

$$N' + J.(M/N) = M/N \implies N' + M/N = M/N \implies N' = M/N$$

$3 \implies 1$
Suppose some element y $\in$ J is not in rad R.Then y $\notin$ m for some maximal ideal m of R.We have m + J = R so, a fortiori, m + J.R = R.From (3) it follows that m = R , a contradiction. QED

Definition. *A ring is said to be von Neumann regular if it satisfies any of the following equivalent conditions*

1. *For any $a \in R$, there exists $x \in R$ such that $a = axa$.*
2. *Every principal left ideal is generated by an idempotent .*
3. *Every principal left ideal is a direct summand of ${}_R R$.*

4. Every finitely generated left ideal is generated by an idempotent.

5. Every finitely generated left ideal is a direct summand of ${}_RR$.

* Wedderburn semisimple $\implies$ Von Neumann Regular $\implies$ J-semisimple
* Von Neumann + Noetherian = Artinian

0.2.1 Quasi-regularity and Circle Decomposition

Definition. *An element z is said to be be right(left) quasi regular , if (1 - z)R(R(1-z)) contains z or equivalently -z .Therefore the condition reduces to the fact that there exists a z' such that*

$$z + z' + z.z' = 0$$

So we define an operation '$\bullet$' in R instead of '.',defined as

$$a \bullet b = a + b - a.b \,\forall\, a, b \in R$$

and an element is said to be right(left) quasi regular if it has a right(left) inverse with respect to this new operation.
A element $z \in R$ is said to be quasi regular if there exists $z' \in R$, such that z' is both the left and right inverse of z w.r.t '$\bullet$'.

Proposition 1. *A quasi-regular right ideal I in a ring R is a subgroup of all quasi regular elements of R.*

Proof. Let z ∈ I and let z' be a right quasi regular inverse of z , then z + z' - z.z' = 0, so that z' = zz' - z ∈ I , hence z' has a right quasi regular inverse z".We have

$$z = z \bullet 0 = z \bullet (z' \bullet z") = (z \bullet z') \bullet z"$$

Hence z $\bullet$ z' = 0 = z' $\bullet$ z and *implies* z is quasi regular. QED

Proposition 2. *Every **nil** ideal is quasi regular.*

Proof. If z is nilpotent , then this implies $z^n = 0$ for some n . Let $z' = -z - z^2 - \ldots - z^{n-1}$ .Then z $\bullet$ z' = 0 = z' $\bullet$ z . Hence z is quasi regular. Hence the proposition. QED

0.2.2 Characterisations of the Jacobson Radical

Definition (I.E. Segal)**.** *A right ideal $I \subseteq R$ is called modular if and only if there exists $e \in R$ such that for all $r \in R$, r-er $\in I$ .The element E is called a left identity modulo.*

Proposition 3. *If I is a proper modular right ideal in r , then I can be embedded inside a maximal(necessarily modular) right ideal .*

Proof. Let e be a left identity modulo I .Consider the class S of right ideals I' such that (i) I' $\supseteq$ I (ii) e $\notin$ I' ,partially ordered by inclusion.S is not empty , since I $\in$ S.Let T be an ordered subclass of S.It is easy to verify that $\cup\{I'|I' \in T\}$ is an upper bound for T .Hence by Zorn's Lemma S has a maximal element I^*.It follows that I^* is a maximal ideal containing I.Since every right ideal containing a modular right ideal is modular, I^* is modular. QED

Claim. *If I is a right modular ideal of R , then I $\supseteq$ R/I.*

Proof. We know that I = $< u >$, where u is a generator of a cyclic module M . I = $< u > \supseteq$ M = R - I = R/I Hence The claim.

Theorem 5. *1. The radical rad R of a ring R is equal to the intersection of all modular maximal right ideals of the ring .*

2. rad R is a quasi regular right ideal and it contains all other quasi regular right ideals .

Proof. (1) If I is a right modular ideal then R/I is simple module and I $\supseteq$ R/I.Hence $\cap\{I|I$; modular maximal right ideal$\} \supset \cap\{$ R/I | I;modular maximal right ideal $\} \supset$ rad R.On the other hand if, M is a simple module R-module then M = $\cap\{< u > |u \in M\}$ and for u $\neq$ 0, $< u >$ is a modular maximal right ideal.Hence we have rad R = $\cap\{$ M — M is simple $\} \supseteq \cap\{I|I$;modular maximal right ideal$\}$. Thus rad R = $\cap\{I|I$;modular maximal right ideal$\}$.

(2) Suppose that r $\in$ rad R and r is not right quasi regular ,then (1-r)R $\neq$ R, and (1-r)R can be embedded inside a right maximal modular ideal I, r $\in$ I .Hence I = U ,which is a contradiction, therefore R rad R is quasi regular.Next let B be any right quasi regular ideal and let z$\in$ B , then zr is right quasi regular for all r $\in$ R.Let M be a simple R-module.Suppose z $\notin$ M, then there exists a u $\in$ M such that ur $\neq$ 0.Thus ur is a strict generator of M and hence there is an a $\in$ R such that ura = u.If R has an identity , then this reads as u(1-ra) = 0.Since (1-ra) has an inverse 1 - r' this leads to u = 0.If R does not have an identity then we can replace this argument by one using quasi inverses.Thus let r' be a right quasi inverse for ra.Then 0 = u - ura - (u - ura)r' = u - u(ra+ r' -rar') = u.This contradicts that ur $\neq$ 0.Hence z $\in$ M,consequently z $\in$ rad R .Hence B $\subseteq$ R .

0.3 Jacobson Radical Under Change of Rings

Theorem 6 (E.Snapper)**.** *Let R be a commutative ring and let R[T] be a polynomial ring over E.Then rad R[T] = Nil (R[T]) = (Nil R)[T].*

Proof. Recall that a ring is called *reduced* if it has no non-zero nilpotent elements .Since R /Nil R is reduced, it is easy to see that (R/Nil R)[T] is reduced .But

$$(\text{R/Nil R})[\text{T}] \cong \text{R[T]}/(\text{Nil R})[\text{T}]$$

so it follows that (Nil R)[T] = Nil(R[T]).Also,Nil(R[T]) $\subseteq$ rad(R[T]),so it only remains to show the reverse condition.For this,we may assume that T is a singleton, say t.Let

$$f(t) = r_0 + \ldots + r_n t^n \in rad(R[t])$$

Then

$$1 + tf(t) = 1 + r_0 + \ldots + r_n t^{n+1} \in U(R[t])$$

Let p be any prime ideal of R .Then the invertibility of the polynomial above in (R/p)[t] implies that each $r_i \in$ p.Since this holds for all prime ideals p $\subset$ R we have $r_i \in$ Nil R , thus f(t) $\in$ (Nil R)[t]. QED

Theorem 7. *Let $R \subseteq A$ be commutative domains such that A is finitely generated as an R-algebra,and R is J-semisimple.Then A is also J-semisimple.*

Proof. It suffices to treat the case where A= R[a].We may assume that a is algebraic over the quotient field K of R ,for otherwise we are done by Snapper's Theorem.Assume that there exists a nonzero element b $\in$ rad A.Then a and b are both algebraic over K.Let

$$\sum_{i=0}^{n} r_i t^i, \qquad \sum_{i=0}^{m} s_i t^i \in R[t]$$

be polynomials of the smallest degrees n,m $\geq$ 1,satisfied,respectively,by a and b .Since A is a domain,

$$s_0 = -\sum_{i=1}^{m} s_i b^i \in radA$$

is not zero ,and so $r_n s_0 \neq 0$.From rad R = 0,we can find a maximal ideal m of R such that $r_n s_0 \notin m$.Upon localising at S = R/m, r_n becomes a unit,so a satisfies a monic equation over $S^{-1}R$;in particular,$S^{-1}A = (S^{-1}R)[a]$ is finitely generated as a module over $S^{-1}R$.By Nakayama's Lemma,

$$(\text{rad } S^{-1}R).S^{-1}A \subset S^{-1}A$$

In particular m.A $\subset$ A .Let m' be a maximal ideal of A containing m.A.Then clearly m' $\cap$ R = m, and sp $s_0 \notin m$ implies that $s_0 \notin m'$, contradicting the fact that $s_0 \in radA$. QED

Theorem 8. *Let $R \subseteq A$ be commutative domains such that rad $R = 0$ and A is finitely generated R-algebra.If A is a field,then so is R ,and A/R is a finite(algebraic) extension.*

Proof. First let us treat the "monogenic" case : A = R[a].Clearly a must be algebraic over the quotient field of R .Let

$$\sum_{i=0}^{n} r_i t^i \in R[t]$$

be a polynomial (with $r_n \neq 0$)satisfied by a ,let m be a maximal ideal in R with $r_n \notin$ m.(Such a ideal exists because rad R =0).As we see m.A $\subset$ A .Since A is a field, the ideal m.A must be 0.Therefore,m itself is zero ,which implies that R is a field.To treat the general case,let A=R$[a_1, \ldots, a_m]$ and write R' = R$[a_1]$.Then rad R' = 0.Invoking an inductive hypothesis(on m),we see that R' is a field and each $a_i (2 \leq i \leq m)$ is algebraic over R'.By the monogenic case,we conclude that R is a field and a_1 is algebraic over R.It follows that a_i is algebraic over R ,and that A/R is a finite field extension. QED

Theorem 9 (Amitsur's Theorem)**.** *Let R be any ring, and $S = R[T]$.Let $J =$ rad S and $N = R \cap J$.Then N is a nil ideal in R, and $J = N[T]$.In particular,if R has no non-zero nil ideal , then S is Jacobson semisimple .*

The proof will be presented in several steps . So lets first prove some results needed prior to the proof of the theorem

Proposition. *N is a nil ideal in R .*

Proof. Let a $\in$ N and $t_0 = t_{i0}$ be one of the variables .Then 1-at is invertible in R[T],say (1-at)g(T) = 1.Setting all variables t_i(i $\neq i_0$) equal to zero we have

$$(1 - at)(a_0 + a_1 t \ldots + a_n t^n) = 1$$

for some $a_j \in R$ .Comparing coefficients ,we have

$$a_0 = 1, a_1 = aa_0 = a, \ldots, a_n = aa_{n-1} = a^n,$$

and $0 = aa_n = a^{n+1}$, as desired . QED

Proposition. *Let $S = R[t]$, $J =$ rad S, and so $a_0, \ldots, a_n \in R$.If $f(t) = a_0 + a_1 t + \ldots + a_n t^n \in J$, then $a_i t^i \in J$ for all i.*

Proof. The concluion is clearly true for n = 0.By induction we may assume the truth of the conclusion (for all rings R) for smaller n.Let p be any prime number > n, and let R_1 be the ring ,

$$R[\theta]/(1 + \theta + \ldots + \theta^{p-1})$$

To simplify notations, we shall write θ for the image of θ in R_1;then $\theta^p = 1$ in R_1.Note that,for any positive integer j < p ,we have

$$p \in (\theta^j - 1)R_1 \tag{7}$$

In fact, in the quotient ring $R_1/(\theta^j - 1)R_1$,we have $\bar{\theta^j} = 1$ and hence $\bar{\theta} = 1$.Therefore ,$1 + \bar{\theta} + \ldots + \bar{\theta^{p-1}} = 0$ implies that $\bar{p} = 0$.Let $S_1 = R_1[t]$ and $J_1 = radS_1$.Since

$$S_1 = S \oplus \theta S \oplus \ldots \oplus \theta^{p-2} S \tag{8}$$

and θ is central in S_1,we have $J_1 \cap S = J$.Now by applying the automorphism t $\rightarrow$ θt onS_1, f(t) $\in$ J $\subseteq$ J_1 leads to f(θt) $\in$ J_1 and hence

$$\theta^n f(t) - f(\theta t) = a_0(\theta^n - 1) + a_1(\theta^n - \theta)t + \ldots + a_{n-1}(\theta^n - \theta^{n-1})t^{n-1} \in J_1. \tag{9}$$

Invoking the inductive hypothesis(overR_1),we have $a_i(\theta^n - \theta^i)t^i \in J_1$ and hence $a_i(\theta^{n-i} - 1)t^i \in J_1$ for any i $\leq$ n-1.We also see that $pa_i t^i \in J_1 \cap S = J$.Applying this argument to another prime q $>$ n , we have also $qa_i t^i \in J$;therefore $a_i t^i \in J$ for all i $\leq$ n-1.Since f(t) $\in$ J ,it follows that $a_n t^n \in J$ as well. QED

Proposition. *In the above proposition, if f(t) $\in$ J, then $a_i \in J$ for all i .*

Proof. Applying the automorphism t $\rightarrow$ t+1 on R[t], the earlier conclusion $a_i t^i \in J$ leads to

$$a_i(1 + t)^n = a_i + na_i t + \ldots + a_i t^n \in J \tag{10}$$

Applying the previous proposition, we see that $a_i \in J$. QED
Proof of the Theorem The desired conclusion J = N[T](N = J $\cap$ R)means that if a polynomial f(T) $\in$ J, then all of its coefficients must belong to J.To see this,we induct on the number m of variables appearing in f.If m = 0,this is clear.If m $>$ 0 , fix a variable t appearing in f.Write T = $T_0 \cup t$(disjoint union) and f(T) = $\sum_i a_i(T_0)t^i$.Applying the previous proposition to R[T] = R[T_0][t].we see that $a_i(T_0) \in J$ for all i.Since the number of variables actually appearing in each $a_i(T_0)$ is m-1, the induction proceeds. QED

0.4 Group Rings and the J-Semisimplicity Problem

0.4.1 Maschke's Theorem

Theorem 10. *Let k be any ring and G be a finite group .Then R = kG is semisimple iff K is semisimple and |G| . 1 is a unit in k .*

Proof. For the "if" part,let W be an R-submodule of a left R-module V.We want to show that W is an R-module direct summand of V .Fix a k-homomorphism

f: V $\rightarrow$ W such that f|W is the identity.(Such a map exists since W is a k-module direct summand of V.)We shall modify f into a map g with the same properties as f ,but such that g is a homomorphism of R-modules.If such a g can be found,then V = W $\oplus$ ker(g) gives what we want .We define g : V $\rightarrow$ V by the following "averaging" device :

$$g(v) := |G|^{-1} \sum_{\sigma \in G} \sigma^{-1} f(\sigma v), v \in V \tag{11}$$

Since g(v) $\in |G|^{-1} \sum_{\sigma \in G} \sigma^{-1}.W \subseteq W$,we may view the k-homomorphism g as from V to W .If v $\in$ W,then

$$g(v) = |G|^{-1} \sum_{\sigma \in G} \sigma^{-1}(\sigma v) = v, \tag{12}$$

so g is the identity on W.Finally,the following computation shows that g is an R-homomorphism: for any $\tau \in G$,

$$\begin{aligned} g(\tau v) &= |G|^{-1} \sum_{\sigma \in G} \sigma^{-1}(f(\sigma\tau.v)) \\ &= |G|^{-1} \sum_{\sigma' \in G} \tau\sigma'^{-1} f(\sigma' v) \\ &= \tau g(v) \end{aligned} \tag{13}$$

For the "only if " part of the theorem ,assume now that R = kG is semisimple .We have a ring homomorphism (the augmentation map)

$$\epsilon : \quad kG \longrightarrow k$$

defined by taking $\epsilon|k = Id_k$ and $\epsilon(G) = 1$.Therefore,as a homomorphic image of kG,k is semisimple . We finish by showing that p dividing $|G|$ is a unit in k.By Cauchy's Theorem in group theory there exists an element in $\sigma \in G$ of order p.Since the semisimple ring R is von Neumann regular ,there exists an element $\alpha \in R$ such that (1 - σ)α(1 $-$ σ) = 1 $-$ σ,from which

$$[1 - (1 - \sigma)\alpha].(1 - \sigma) = 0$$

By the lemma below, we can write

$$1 - (1 - \sigma)\alpha = \beta.(1 + \sigma + \ldots + \sigma^{n-1})$$

for some $\beta \in$ R.Applying the augmentation map ϵ , we have $1 = \epsilon(\beta)$.p, so p = p.1 is invertible in k, as desired. QED

We now prove the required lemma

Lemma 1. *For $r \in R = kG$,and $\sigma \in G$ of order p,r.(1 - σ) = 0 iff $r \in R.(1 + \sigma + \ldots + \sigma^{p-1})$*

Proof. We need only prove the " only if " part.Let r = $\sum_{\tau \in G} r_\tau \tau$.We shall induct on the number n of $\tau^{'s}$ occurring in r with nonzero coefficients .If n = 0 then r = 0 and we are done .Otherwise,look at some τ with $r_\tau \neq 0$.Since ,

$$r = r.\sigma = r.\sigma^2 = \ldots,$$

the group elements $\tau, \tau\sigma, \ldots, \tau\sigma^{p-1}$ all appear in r with the same coefficient r_τ.Therefore

$$\begin{aligned} r &= r_\tau(\tau + \tau\sigma + \ldots + \tau\sigma^{p-1}) + (\text{K-combination of other group elements}) \\ &= r_\tau(1 + \sigma + \ldots + \sigma^{p-1}) + r'(say) \end{aligned} \tag{14}$$

Since r.(1 - σ) = 0 implies that r'.(1 - σ) = 0,the proof proceeds by induction. QED

Proposition. *Let $k \neq 0$ be any ring , and G be an infinite group.Then the group ring R = kG is never semisimple.*

Proof. For the augmentation map ϵ : kG $\longrightarrow$ k defined above ,Let U := ker(ϵ) be the " augmentation ideal ".Assuming R = kG is semisimple,we have R = U $\oplus$ B ,where B $\subset$ R is a suitable left ideal.Write

$$\text{U} = \text{R.e and B} = \text{R.f}$$

where e,f are idempotents such that e + f = 1.Clearly e,f are not zero .We have U.f = Re.f = 0,so ($\sigma - 1$)f = 0,i.e.,f = σf,for any $\sigma \in$ G .Let $\tau \in$ G be a group element which appears in f with a nonzero coefficient.Then $\sigma\tau$ appears in f with the same coefficient,for any $\sigma \in$ G .This means that f involves all group elements of G; since G infinite,this contradicts the definition of group ring. QED

Theorem 11 (Amitsur's Theorem)**.** *Let K be a non algebraic field extension of $\mathbb{Q}$.Then for any group G, the group ring kG is J-semisimple*

Proof. Let F = $\mathbb{Q}(\{x_j\})$,where $\{x_j\}$ is a non empty transcendence basis for K/$\mathbb{Q}$.Note that the sclar extension $\mathbb{Q}G \otimes_{\mathbb{Q}}$F is just FG.Let J = rad FG.So N = J $\cap \mathbb{Q}G$ is a nil ideal of $\mathbb{Q}$G and J = N $\otimes_{\mathbb{Q}}$F = N.F.However, $\mathbb{Q}$G has no non zero nil left ideal; hence N = 0 and so J = 0.This shows that FG is J-semisimple.Since we are in characteristic zero, K/F is a separable algebraic extension.Therefore,the scalar extension FG $\otimes_F$ K = KG is also J-semisimple. QED

Proposition. *Let k be a commutative reduced ring of prime characteristic p > 0.Let G be any p'-group .Then R = kG has no non zero nil left ideals.*

Proof. Assume that R has a non zero nil left ideal B ,say

$$0 \neq \beta = \sum \beta_g g \in B$$

After left multiplying with β with a suitable group element ,we may assume that tr(β) = $\beta_1 \neq 0$.We claim that $tr(\beta_p) = tr((\beta))_p$.If so ,then by iteration,

$$tr(\beta^{p^n}) = (tr(\beta))^{p^n} \neq 0$$

for every n ,and we get the desired contradiction .To show our claim,note that

$$tr(\beta^p) = tr\left(\left(\sum \beta_g g\right)^p\right) = \sum \beta_{g_1}\beta_{g_2}\ldots\beta_{g_p} \tag{15}$$

where the sum is over the set S of ordered p-tuples $(g_1, g_2 \ldots, g_p)$ of group elements such that $g_1 \ldots g_p = 1$.The cyclic group H = $< \sigma >$ of order p acts on S by

$$\sigma * (g_1, g_2, \ldots, g_p) = (g_2, \ldots, g_p, g_1) \tag{16}$$

The H-orbits on S have cardinality either 1 or p .For an orbit of cardinality p ,since all the p-tuples in the orbit make the same contribution to $tr(\beta^p)$,the total contribution is a multiple of p,and therefore is zero .Now look at a singleton orbit $H * (g_1, \ldots, g_p)$.We must have $g_1 = g_2 = \ldots = g_p$ and hence $g_1^p = 1$.Since G is a p'-group,we have $g_1 = g_2 = \ldots = g_p = 1$.Therefore,there is a unique singleton orbit in S and its contribution to $tr(\beta^p)$ is β^p,as claimed.
QED

Proposition. *Let K/F be an algebraic extension of fields of characteristic p, and let G be a p'-group.If FG is J-semisimple,so is KG.*

Proof. Fist let us assume that [K :F] = N $< \infty$
Therefore

$$(rad(KG))^n \subseteq (radFG).K$$

and,rad FG = 0.Thus ,rad KG is a nilpotent ideal .By the above proposition,therefore, rad KG = 0.Now drop the assumption that [K :F] < n ∞.Given any element $\alpha \in$ KG, we can find a field $K_0 \subseteq K$ of finite degree over F such that $\alpha \in K_0$G.Therefore,we have

$$\alpha \in K_0G \cap rad\, KG \subseteq rad\, K_0G \tag{17}$$

But by the case that we have already treated , rad $K_0G = 0$ and so $\alpha = 0$.
QED

Theorem 12 (Passman's Theorem)**.** *Let K be a non algebraic field extension of $\mathbb{F}_p$ (the field of p elements).Then for any p'-group G, the group ring KG is J-semisimple.*

Proof. As before , let $\{x_j\}$ be a non empty transcendence basis for K/$\mathbb{F}_p$,and let F = $\mathbb{F}_p(\{x_j\})$.By one of the previous propositions $\mathbb{F}_p$G has no non zero nil left ideals.Arguing as in the proof of the previous proposition ,we see that FG is J-semisimple.Applying the previous proposition to the algebraic extension K/F, it follows that KG is also J semisimple. QED

Theorem 13. *Let k be a domain and (G,<) be an ordered group.Then A = kG has only trivial units and is a domain.If $G \neq \{1\}$,A is J -semisimple .*

Proof. Consider a product $\alpha\beta$ where

$$\begin{aligned} \alpha = a_1g_1 + \ldots + a_mg_m, g_1, \ldots, g_m, a_1 \neq 0 (1 \leq i \leq m), \\ \beta = b_1h_1 + \ldots + b_nh_n, h_1, \ldots, h_n, b_j \neq 0 (1 \leq j \leq n), \end{aligned} \tag{18}$$

W e have $g_1h_1 \leq g_ih_j$,with equality iff i = j.Thus, the smallest group element appearing in $\alpha\beta$ is g_1h_1(with non-zero coefficient a_1b_1),and similarly the " largest " one is g_mh_n(with nonzero coefficients a_mb_n).In particular ,$\alpha\beta \neq 0$, and if $\alpha\beta = \beta\alpha = 1$, we must have m = n = 1,so $\alpha = a_1g_1, \beta = b_1h_1$, with $a_1b_1 = b_1a_1 = 1$ in k and $g_1h_1 = 1$ in G.This proves that A is a domain, and that A has only trivial units.The last statement of the theorem then follows .

Theorem 14. *Let k be a field and G be an abelian group.*

1. *If char k = 0,then A = kG is J-semisimple.*
2. *If char k = p,then A = kG is J-semisimple iff G is a p'-group.*

Proof. First assume that char k = p and A is J-semisimple.Then G must be a p'-group for if x ∈ G has order p,then $((x-1)A)^p = 0$ and rad A ⊇ (x-1)A $\neq 0$.Now assume that char k = 0, or that char k = p and G is a p'-group.To show that kG is J-semisimple,we may assume that G is finitely generated .For, if $\alpha \in$ rad kG,there exists a finitely generated subgroup $G_0 \subseteq$ G such that $\alpha \in$ kG_0.Then $\alpha \in kG_0 \cap$ rad kG ⊆ rad kG_0,so it suffices to show that rad k$G_0 = 0$.If G is finitely generated ,we can write G = $G_t \times H$ where G_t is the torsion subgroup of G and H is a free abelian group of finite rank.As is easily verified,A = kG is isomorphic to the group ring RH where R = kG_t.Since G_t is finite and char k does not divide its order, Maschke's Theorem implies that R is semisimple ,and so R ≅ $k_1 \times \ldots \times k_m$ where the k_i's are suitable fields.We have an isomorphism

$$A \cong RH \cong (k_1 \times \ldots \times k_m)H \cong k_1H \times \ldots \times k_mH$$

so it sufiicces to show that k_iH is J-semisimple.But H is an ordered group since H ≅ $\mathbb{Z} \times \ldots \times \mathbb{Z}$ can be given the lexicographic ordering .Therefore, the J-semisimplicity of k_iH follows. QED

0.5 Introduction to Representation Theory

0.5.1 Modules Over Finite Dimensional Algebras

Let $\bar{R} = B_1 \times \ldots \times B_t$ be the decomposition of $\bar{R}$ into simple components and let $M_i (1 \leq i \leq r)$ be the unique simple left module over $B_i's$. Then

$$\bar{R} = \mathbb{M}_{n_1}(D_1) \times \ldots \times \mathbb{M}_{n_r}(D_r)$$

$$_R\bar{R} \cong n_1 M_1 \oplus \ldots \oplus n_r M_r (19)$$

Proposition. *In this notation we have*

1. $dim_k M_i = n_i dim_k D_i$
2. $dim_k R = dim_k\ rad\ R + \sum_{i=1}^{r} n_i^2 dim_k D_i$
3. *The natural map* $R : \to End(M_i)_{D_i}$ *is onto .*

If $D_i = \mathrm{k}$, the last part of the proposition amounts to this lemma

Lemma (Burnside's Lemma)**.** *Let M be a finite-dimensional right k-vector space and A be a k-subalgebra of End(M_k)such that M is simple as a left A-module.If End($_A M$) = k,then A = End(M_k).*

Proof. By Schur's Lemma the D_i's are finite dimensional k-division algebras.The easiest case is when k is an algebraically closed field.In this case D_i must be k itself (for, if d $\in D_i$,then k[d] is a finite field extension of k, and hence d must be in k).Consequently we have

$$\bar{R} = \mathbb{M}_{n_1}(k) \times \ldots \times \mathbb{M}_{n_r} \quad (20)$$

and simplifies to $dim_k M_i = n_i$ and

$$dim_k R = dim_k rad R + \sum_{i=1}^{r} n_i^2 \quad (21)$$

Also the condition End($_A M$) = k is automatic and therefore can be removed:this gives in fact the Burnside's Theorem in its original form.

Theorem 15. *Let R be a k-algebra and let M be a simple left R-module with* $dim_k M < \inf$*.The following statements are equivalent :*

1. *End($_R M$) = k.*
2. *The map $R \to End(M_k)$ expressing the R-action on M is surjective.*
3. *For any field extension $K \supseteq k$, M^K is a simple R^K-module.*

4. *There exists an algebraically closed field $E \supseteq k$ such that M^E is a simple R^E -module.*

If one (and hence all) of these conditions holds,we say that M is an absolutely simple (or absolutely irreducible) R-module.

Proof. Clearly 3 $\implies$ 4 , so it suffices to show that

$$4 \implies 1 \implies 2 \implies 3$$

Assume 4.Since E is algebraically closed,this implies that $Hom_{R^E}(M^E, M^E) \cong$ E and therefore $Hom_R(M, M) \cong$ k.
Next, 1 $\implies$ 2 follows from the Burnside's lemma.
Now assume (2).To prove (3),we may replace R by End(M_k).If $M_k = k^n$,we can then identify R with the full matrix algebra $\mathbb{M}_n(k)$.With these identifications,we have $M^K = K^n$ and $R^K = \mathbb{M}_n(K)$,so M^K is a left simple R^K-module,as desired. QED

Definition. *Let R be a finite dimensional k-algebra .We say that a field K $\supset$ k is a splitting field for R if every left irreducible R^K-module is absolutely irreducible.*

Theorem 16. *In the previous notation ,K is a (left) splitting field for R iff $R^K/rad\ (R^K)$ is a finite direct product of matrix algebras over K.*

Proof. To simplify notation , we take K = k .If each irreducible R-module M_i is absolutely irreducible ,then , each $D_i = End_R(M_i)$ is k so R/rad R is a finite direct product of matrix algebras over k.The converse is proved similarly. QED

Corollary 0.3. *A k-algebra R splits over k iff*

$$dim_k R = dim_k(radR) + \sum (dim_k M_i)^2, \tag{22}$$

where $\{M_i\}$ is a full set of simple left R-modules.

0.6 Representation of Groups

Let k be a field and G be a finite group such that char k does not divide $|G|$ and let $M_1, \ldots, M_r$ be a complete set of simple left kG-modules;let $D_i = End(_{kG}M_i)$ and $n_i = dim_{D_i} M_i$.Then we have

Theorem 17. 1. *$kG/rad\ kG \cong \mathbb{M}_{n_1}(D_1) \times \ldots \times \mathbb{M}_{n_r}(D_r)$*

2. *As a left kG-module,$kG/rad\ kG \cong n_1 M_1 \oplus \ldots \oplus n_r M_r$.*

3. *$dim_k M_i = n_i dim_k D_i$.*

4. *$|G| = dim_k(rad\ kG) + \sum_{i=1}^r n_i^2 dim_k D_i$.*

Definition. *We say that a field k is a splitting field for G if the group algebra kG splits over k .*

Theorem 18. *Let k be any field,and G be any group.Then some finite extension $K \supseteq k$ is a splitting field for G*

Proof. Let K_0 be the prime field of k, and $\bar{K}$ be the algebraic closure of k.Since k_0 is perfect , it implies that a finite extension $k_1 \supseteq k_0$ in $\bar{k}$ is a splitting field for G .Let K = k.k_1,the field composition being formed in $\bar{k}$.Clearly K is a finite extension of k,and by k_1 being a splitting field for G implies the same for K . QED

Theorem 19. *Let k be a field of characteristic $p \geq 0$,and G be a finite group.Then any normal p-subgroup $H \subset G$ acts trivially on any simple left kG-module.Thus,simple left kG-modules are the same as simple left k[G/H]-modules.(In particular,if G is a p-group,then the only simple left kG -module is k , with trivial G-action).*

To prove this theorem we would be using another very handy theorem

Theorem 20 (Clifford's Theorem)**.** *Let k be any field , and H be a normal subgroup of a (possibly infinite) group G.If V is a simple left kG-module,then ${}_{kH}V$ is a semisimple kH-module .*

Proof. Let M be a simple kH-submodule of V .For any g ∈ G,g.M is also a kH-submodule of V since

$$h(gM) = g(h^g M) = gM \tag{23}$$

where $h^g = g^{-1}hg \in H$.Moreover,gM is a simple kH-module because if M' is a kH-submodule of it,$g^{-1}M'$ would be a $kH - submodule$ of M .Now consider V': $= \sum_{g \in G} gM$.This is semisimple kH- module,and since it is also a kG-submodule of V,we have V' = V.

Proof of the main Theorem By Clifford's Theorem we are reduced to proving that H acts trivially on the any simple kH-module M .We do this by induction on $|H|$,the case $|H| = 1$ being trivial. If $|H| > 1$, let $h \neq 1$ be an element in the center of H , say of order p^n.*Since*

$$(h-1)^{p^n} = h^{p^n} - 1 = 0 \in kH \tag{24}$$

h - 1 acts as a nilpotent transformation on M,so its kernel is nonzero.Let $M_0 = \{m \in M | hm = m\} \neq 0$.This is kH-submodule of M and so $M_0 =$ M.Therefore, M may be viewed as a simple k[H/$< h >$]-module,and we are done by induction. QED

Corollary 0.4. *Let k be a field of characteristic $p > 0$,and G be a finite group .For $h \in G$, the following are equivalent*

1. $h \in O_p(G)$.

2. *h acts trivially on all simple left kG-modules.*

3. *h - 1 ∈ rad(kG).*

Proof. 2 $\implies$ 3 is trivial and 1 $\implies$ 2 follows from the previous theorem since $O_p(G)$is normal.Now assume (2).By considering a composition series of the left regular module kG, we see that h - 1 acts as a nilpotent transformation on kG.Thus, for a sufficiently large integer n ,

$$(h-1)^{p^n} = h^{p^n} - 1 = 0 \in kG \tag{25}$$

i.e, the order of h is a power of p.Now let H be the set of all elements h of G satisfying (2).This H is easily seen to be a normal subgroup of G , and what we did above shows that H is a p-group .Thus H $\subseteq O_p(G)$ and we are done . QED

Corollary 0.5 (Wallace)**.** *Let k be a field of characteristic p,and G be a finite group with a normal p-Sylow group H .Then*

$$rad\, kG = \sum_{h \in H} kG.(h-1) \tag{26}$$

with dim_k rad kG =[G:H](|H| - 1)

Proof. Since (h - 1)g = g($h^p - 1$)for any g ∈ G ,the left ideal

$$U = \sum_{h \in H} kG.(h-1) \tag{27}$$

is in fact an ideal, and this lies in rad kG .The quotient kG/U is easily seen to be isomorphic to k[G/H].Since p = char k is not a divisor of [G : H], k[G/H] is semisimple by Maschke's theorem.Therefore we have rad kG = U and

$$dim_k rad\, kG = |G| - |G/H| = [G:H](|H| - 1) \tag{28}$$

QED

PART - 2 - LOCAL FIELDS

0.7 Localisation

Let R be an integral domain. This means R is a commutative ring with identity having no zero divisors. Let S be a subset of R which does not contain zero and which contains the product of any two elements in S. A set satisfying these conditions is called a *multiplicative set* in R.

Proposition 4. *There is a ring R_s which contains R as a subring (up to isomorphism) and such that each element of S has a multiplicative inverse in R_s.*

Proof. Let us first consider the collection of all pairs (r, s) in $R \times S$. Call two such pairs (r, s) and (q, t) equivalent if qs = rt.This is an equivalence relation. Let r/s denote the equivalence class containing (r, s). By definition of the equivalence class we see that r/s = rt/st for any tin S. Let $R_s = \{\text{r/s} \mid \text{r} \in \text{R}, \text{s} \in \text{S}\}$. Addition and multiplication are defined for elements of R_s by the rules

$$\begin{aligned} r/s + r'/s' &= (rs' + r's)/ss' \\ r/s.r'/s' &= rr'/ss' \end{aligned} \tag{29}$$

The ring R_s constructed in the proof has the following universal property: If ϕ is a homomorphism of R into a ring T such that every element in ϕ(S) has an inverse in T, then ϕ has a unique extension to a homomorphism from R_s into T. The extended map is defined by $\phi(\text{r/s}) = \phi(\text{r})\phi(\text{s})^{-1}$ This kind of reasoning shows the ring R_s is characterized as the smallest ring containing R and inverses for the elements of S.

Definition. *The ring R_s is called the localization of R at S.*

Proposition 5. *Let R be an integral domain and S a multiplicative set in R. There is a one-to-one correspondence between the prime ideals of R_s and the prime ideals of R which have empty intersection with S. Under the correspondence, a prime ' p ' of R is associated with the ideal ' pR_s ' in R_s.*

Proof. Let Q be a prime ideal in R_s. From the definition it is immediate that B = Q ∩ R is a prime ideal of R. Then BR_s is an ideal of R_s contained in Q. We show these are equal. Let q/s be any element in Q with q in R and s in S. Then q = (q/s)s is in R ∩ Q = B. Thus q/s is in BR_s since q(1/s) = q/s, q in B, 1/s in R_s. So far we have proved that every prime ideal in R_s has the form Q = BR_s with B = Q ∩R_s uniquely determined by Q. Since every element in S has an inverse in R_s we know Q ∩ S is empty. Thus B ∩ S is empty. Now suppose we start with the prime ideal B of R which has no elements in S. Let Q = BR_s. This is an ideal of R_s which we shall prove is prime. Suppose a, b are elements in R_s with ab in Q, then ab = x/s with some x in B and some s in S. Suppose a = r_1/s_1 , b = r_2/s_2 with r_1, r_2 in R and s_1, s_2 in S. We have

$r_1 r_2 s = x s_1 s_2$ belongs to B. Thus one of the elements r_1 , r_2 or s is in B since B is prime.Also s is not in B by choice of B. Thus $r_1 or r_2$ belongs to B and so $a = r_1/s_1 or b = r_2/s_2$ is in Q. Thus Q is prime. Now finally we prove Q $\cap$ R = B. If u is in Q $\cap$ R then u = x/s with x in B because Q = BR_s. But u also belongs to R and so x = us implies u or s is in B. Since s is not, we have u is in B. Hence the correspondences B $\rightarrow$ BR_s and Q $\rightarrow$ Q $\cap$ R are inverses of one another and the proposition is proved.

Example - Let B be a prime ideal in the domain R and let S = $\{r | r \notin B\}$ = R - B. The definition of prime ideal is equivalent with the assertion that S is a multiplicative set. Then R_s can be identified with $\{a/b | a, b \in R, b \notin B\}$.

0.8 Discrete Valuation Rings

Definition. *A ring A is called a discrete valuation ring if it is a principal ideal domain that has a unique non-zero prime ideal m(A). [Recall that an ideal p of a commutative ring A is called prime if the quotient ring A/p is an integral domain.)*

The field A/m(A) is called the *residue field* of A. The invertible elements of A are those elements that do not belong to m(A); they form a multiplicative group and are often called the units of A (or of the field of fractions of A). In a principal ideal domain, the non-zero prime ideals are the ideals of the form πA, where π is an irreducible element. The definition above comes down to saying that A has one and only one irreducible element, up to multiplication by an invertible element; such an element is called a uniformizing element of A . The non-zero ideals of A are of the form m(A) = π^nA, where π is a uniformizing element. If x $\neq$ 0 is any element of A, one can write x = π^nu, with n $\in \mathbb{N}$ and u invertible; the integer n is called the **valuation**(or the order) of x and is denoted v(x); it does not depend on the choice of π. Let K be the field of fractions of A, $K^\times$ be the multiplicative group of non-zero elements of K. If x = a/b is any element of $K^\times$, one can again write x in the form π^nu, with n $\in$ Z this time, and set v(x) = n. The following properties are easily verified:

1. The map v: K* $\to \mathbb{Z}$ is a surjective homomorphism
2. One has v(x + y) $\geq$ Inf((v(x),v(y)) (We take the convention that v(0) = $+\infty$

Proposition 6. *Let K be a field, and let v: $K^\times \to \mathbb{Z}$ be a homomorphism having properties (1) and (2) above. Then the set A of x $\in$ K such that v(x) $\geq$ 0 is a discrete valuation ring having v as its associated valuation.*

Proof. Indeed, let ,π be an element such that v(π) = I. Every x $\in$ A can be written in the form x = π^nu, with n = v(x), and v(u) = 0,i.e., u invertible. Every nonzero ideal of A is therefore of the form ,π^nA, with n $\geq$ 0, which shows that A is indeed a discrete valuation ring.
A valuation v of k is called discrete if v($k^\times$) is a discrete subgroup of R^+, that is , if v($k^\times$) = $\mathbb{Z}$ β = { n β | n = 0, $\pm$1, $\pm$2, ... } for some real number $\beta > 0$. If β = 0, then v is the trivial valuation v_0 . When β = 1,that is, when v($k^\times$) = $\mathbb{Z}$ = { O , $\pm$1 , $\pm$2 , ... }, v is called a *normalized*, or normal, valuation of k. It is clear that a valuation v of k is discrete but non-trivial if and only if v is equivalent to a normalized valuation of k.
Let k' be an extension field of k, and v' a valuation of k'. Let v'|k denote the function on k, obtained from v' by restricting its domain to the subfield k. Then v'|k is a valuation of k, and we call it the restriction of v' to the subfield k. On the other hand, if v is a valuation of k, any valuation v' on k' such that

v'|k = v
is called an extension of v to k'. When v' on k' is given, its restriction v'| k is always a well-determined valuation of k. However, given a valuation v on k, it is not known a priori whether v can be extended to a valuation v' of k'. The study of such extensions is one of the main topics in the theory of valuations.
Let v'|k = v as stated above. Then the v'-topology on k' induces the v-topology on the subfield k so that k is a topological subfield of k '. Let o', B', and T' denote the valuation ring, the maximal ideal, and the quotient field of v', respectively:

$$\begin{aligned} o' &= \{x' \in k' | v'(x') \geq 0\} \\ B' &= \{x' \in k' | v'(x') > 0\} \\ T' &= o'/B' \end{aligned} \tag{30}$$

Then o = B' ∩ k, B = B' ∩ k = B' ∩ o T = o/p = o/(B' ∩ o) = (o + B')/B' ⊆ o'/B' = T' Thus the residue field f of v is naturally embedded in the residue field k' of v'. On the other hand, v'|k = v also implies v($k^\times$) ⊆ $v'(k'^\times)$ ⊆ R^+ . Let,

e = e(v'/v) = [v'(k'$^\times$) : $v(k^\times)$] and f = f(v'/v) = [T' :T] where [v'(k'$^\times$) : $v(k^\times)$] is the group index and [T' : T] is the degree of the extension T', e and f are called the **ramification index** and the **residue degree** of v'|v, respectively.

0.9 Complete-Fields

Let v be a valuation of a field k. We say that k is a complete field with respect to v, or, simply, that (k, v) is a complete field, if v is a complete, normalized valuation of k.

Example 1- Let p be a prime number and let v_P be the p-adic valuation of the rational field Q . Since v_P is a normalized valuation, the completion (k', v') of (Q, v_P) is a complete field. k' is nothing but the classical p-adic number field Q_p, and v', often denoted again by v_p , is the standard p-adic valuation of (Q_p, v_p), the valuation ring is the ring $\mathbb{Z}_p$ of p-adic integers and the maximal ideal is p$\mathbb{Z}_p$ so that the residue field is $\mathbb{Z}_p/p\mathbb{Z}_P = \mathbb{F}_p$, the prime field with p elements. Note that $v_p(p) = 1$.

Example 2- Let F be a field, T an indeterminate, and F((T)) the set of all formal Laurent series of the form

$$\sum_{-\infty<<n} a_n T^n, a_n \in F \tag{31}$$

where -∞ << n indicates that there are only a finite number of terms a_nT^n with n < 0, $a_n \neq 0$. Then k = F((T)) is an extension field of F in the usual addition and multiplication of Laurent series. Let v(O) = + ∞ and let v(x) = i if

$$x \neq 0, x = \sum_{n=i}^{\infty} a_n T^n, a_i \neq 0 \tag{32}$$

Then one checks easily that (k, v) is a complete field. The valuation ring is the ring F[[T]] of all (integral) power series in T over F, the maximal ideal is TF[[x]], the residue field is F[[T]]/TF[[T]] = F, and v(T) = 1

0.9.1 Finite Extensions of Complete Fields

A complete field (k', v') is called an extension of a complete field (k, v) if k' is an extension field of k and if the restriction of v' on k is equivalent to v:

$$k \subseteq k'$$

$$and \text{ v'|k} \sim v$$

(33)

In such a case, we shall also say that (k', v') is a *complete extension* of (k, v), or, in short, that k' I k is an *extension of complete fields.*
Let (k, v) and (k', v') be as above and let

$$\mu = v'|k, e = e(v'/\mu), f = f(v'/\mu) \tag{34}$$

e and fare then denoted also by e(k'/k) and f(k'/k), respectively, and they are called the ramification index and the residue degree of the extension k'Ik of complete fields:

$$e = e(k'/k) = e(v'/\mu), f = f(k'lk) = f(v'/\mu) \tag{35}$$

Let $\mu = \alpha$v, $\alpha > 0$ Then $\mu(k^\times) = \alpha v(k^\times) = a\mathbb{Z}$ so that
e = $[v'(k^\times) : \mu(k^\times)] = [\mathbb{Z} : \alpha\mathbb{Z}] = \alpha.$
Therefore

Lemma. *Let (k', v') be a complete extension of a complete field (k, v). Assume that f(k'|k) is finite. Then k'|k is a finite extension and*

$$[k' : k] = ef, e = e(k'/k), f = f(k'/k) \tag{36}$$

Proof. Let $w_1, \ldots, w_n$ be a basis of T' over T and let $\epsilon_i \in$ B' be an element, taken from the residue class w_i in T' = o'/B'.Let A be a complete set of representatives of T = o/B in o, containing 0,and let

$$A' = \{\sum_{i=1}^{f} a_i\epsilon_i | a_1, \ldots, a_f \in A\} \tag{37}$$

Then A' is a complete set of representatives of T' = o'/'B' in o'. Fix a prime element π of k and a prime element π' of k': v(π) = v'(π') = 1. Writing each integer m in the form

$$m = te + j, t = 0, \pm1, \pm2, \ldots, j = 0, 1 \ldots, e - 1 \tag{38}$$

we put

$$\pi'_m = \pi^t \pi'^j$$
Since v'|k = ev, we then have

$$v'(\pi'_m) = et + j = m$$
and we see that each x' $\in$ k' can be uniquely written in the form

$$x' = \sum_{\infty<<m} a'_m \pi'_m \quad with \;\; a'_m \in \quad A' \tag{39}$$

$$a'_m = \textstyle\sum_{i=1}^{f} a_{i,m}\epsilon_i \qquad a_{i,m} \in A.$$

Then,

$$x' = \sum_m \sum_{i=1}^{f} a_{i,m}\epsilon_i \pi'_m = \sum_{i,j} x_{ij}\epsilon_i \pi', 1 \leq i \leq f, 0 \leq j \leq e \tag{40}$$

where $x_{ij} = \sum_{-\infty<<i} a_{i,te+j}\pi' \in k$
Thus every x' in k' is a linear combination of
$\eta_{ij} = \epsilon_i \pi'^j 1 \leq i \leq f, 0 \leq j \leq e$,with coefficients in k .However the elements η_{ij} are linearly independent over k. Therefore [k' : k] = ef < ∞.

Proposition 7. *Let (k, v) be a complete field, and k' a finite extension of k. Then there exists a unique normalized valuation v' on k' such that*

$$v'|k \sim v$$

(41)

(k', v') is then a complete extension of (k, v) and

$$[k' : k] = ef, fore = e(k'/k), f = f(k'/k),$$

v'(x') = 1/f v($N_{k'/k}(x')$)for$x' \in k'$.
(42)

where N is the Norm map from k' to k.

Proof. We know that there exists a unique valuation μ on k' such μ'|k $\sim$ v Furthermore, such a valuation μ is complete and it satisfies,

$$\mu'(x') = \frac{1}{n} v(N_{k'/k}(x'))for x' \in k' \tag{43}$$

with n= [k' :k].Since v($k^\times$) = $\mathbb{Z}$. It follows that

$$\mu(k^\times) \subseteq \tfrac{1}{n}\mathbb{Z}$$

so that μ' is discrete. Hence, there exists a unique normalized valuation v' on k' such that v'$\sim \mu$'. It then follows that v' is the unique normalized valuation on k' such that v'|k $\sim$ v. As μ is complete, v' is also complete, and (k', v') is a complete extension of (k, v). Let $w_l, \ldots, w_s$ be any finite number of elements in f' that are linearly independent over f and let ϵ_i be an element in the residue class w_i, $1 \leq i \leq s$, in T' = o'/B'. Then, we know that $\epsilon_l, \ldots, \epsilon_s$

are linearly independent over k so that s =[k' :k]. This implies that f = f(k'|k)= [T' : T] $\leq$ n $< \infty$. Therefore, n = ef. Now, since v'$\sim \mu'$ that is, I, v' = $\alpha\mu'$, $\alpha > 0$, we have

$$v'(x') = \beta v(N_{k'/k}(x'))\ \ for\ \ x' \in\ k'$$

with $\beta = \alpha/n > 0$. For x in k , this implies
v'(x) = $\beta v(x^n) = \beta n v(x)$(44)
However, v'(x) = ev(x).As n = ef , it follows that β =1/f, so that

$$v'(x') = \tfrac{1}{f} v(N_{(k'/k}(x'))\ \ for\ \ x' \in k'$$

Now, let $\{\alpha_1, \ldots, \alpha_n\}$ denote the elements
$\eta_{ij} = \epsilon_i \pi'^j\ \ 1 \leq i \leq f, 0 \leq j \leq e.$
arranged in some order.We saw that ef = [k' :k] = n and that $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of k' over k. Let

$$x' = \textstyle\sum_{i=1}^{n} x_i \alpha_i, \qquad x_i \in k$$

Then it follows that for any integer r,

$$v'(x') \geq re \Leftrightarrow v(x_i) \geq r \text{ for i = 0,1, ...,n}$$

For r = 0, this means that $\{\alpha_1, \ldots, \alpha_n\}$ is a free basis of the o-module : o' = $\{o\alpha_1, \ldots, o\alpha_n\}$. Let k^n (resp. o^n) denote the direct sum of n copies of k (resp. o) and let k^n be given the product topology of the v-topology on k. The above equivalence then shows that the k-linear map

$$k^n \to k$$
$$(\mathrm{x}_1, \ldots, x_n) \to x' = \textstyle\sum_{i=1}^{n} x_i \alpha_i$$

is a topological isomorphism and it induces a topological o-isomorphism
$o^n \to o' = o\alpha_1 \oplus \ldots \oplus o\alpha_n.$

Proposition 8. *Let (k, v) and (k', v') be the same as in the previous Proposition , and let o and o' be their valuation rings. Then the trace map and the norm map of the finite extension k' /k:*

$$Tr_{k'/k} : k' \to k \qquad N_{k'/k} : k' \to k$$

(45)

are continuous in the v-topology of k and the v'-topology of k', and

$$Tr_{k'/k}(o') \subseteq o \quad \text{ and } \quad N_{k'/k}(o') \subseteq o \tag{46}$$

Proof. Let x' $\in$ k' and

$$x'\alpha_i = \sum_{j=1}^{n} x_{ij}\alpha_j x_{ij} \in k.$$

for the basis $\{\alpha_1, \ldots, \alpha_n\}$ stated above. Then x_0 depends continuously on x' $\in$ k'. Since $Tr_{k'/k}(x')and N_{k'/k}(x')$ are the trace and the determinant of the n $\times$ n matrix (x_{ij}), respectively, the first half is proved. If x' $\in$ 0', then $x_{ij} \in$ o for all i, j. Therefore, the second half is also clear.

Now, let α' be an ideal of (k', v') that is, an o'-submodule of k' different from $\{0\}$, k'. We define the norm $N_{k'/k}(\alpha')$ of to be the o-submodule of k generated by $N_{k'/k}$(x') for all x' $\in \alpha'$. Then $N_{k'/k}(\alpha')$ is an ideal of (k, v) and it follows from the formula for v'(x') that if $\alpha' = B'^n, m \in \mathbb{Z}$, then

$$N_{k'/k}(\alpha') = B'^{mf} \quad where \quad f = f(k'/k)$$
$$\implies N_{k'/k}(o') = o \quad and \quad N_{k'/k}(B') = B^f.$$

0.10 Local-Fields

A complete field, is called a **local field** when its residue field is a finite field.

0.10.1 General-Properties

Let (k, v) be a local field. By the definition, (k,v) is a complete field and its residue field T = o/p is a finite field. Let q be the number of elements in T that is,

$$T = \mathbb{F}_q$$

$\mathbb{F}_q$ denoting, in general, a finite field with q elements. When f is a field of characteristic p namely, when q is a power of a prime number p ,the local field (k, v) is called a p-field. This happens if and only if

$$B.o \subset B \text{ that is } \mathrm{v}(\mathrm{p}.1_k) > 0$$

where 1_k denotes the identity element of the field k. Hence it follows that if (k, v) is a p-field, then the characteristic of the field k is either 0 or p.
Example - 1 Let $\mathbb{Q}_p$ be the p-adic number field, and v_p the p-adic valuation on Q_p. Then $(\mathbb{Q}_p, v_p)$ is a complete field and its residue field is

$$T = \mathbb{Z}_p/p\mathbb{Z} = \mathbb{F}_p$$

Hence $(\mathbb{Q}_p, v_p)$ is a p-field of characteristic O. On the other hand, let F be any finite field of characteristic p; for example, F = F_p . Let k = F((T)) be the field of formal Laurent series in T with coefficients in F, and let VT be the standard valuation of k . Then (k, v_T) is a complete field and its residue field is

$$\mathrm{T} = \mathrm{o}/\mathrm{B} = \mathrm{F}[[\mathrm{T}]]/\mathrm{TF}[[\mathrm{T}]] = \mathrm{F}$$

Therefore (k, v_T) is a p-field of characteristic p..

Proposition 9. *Let (k, v) be a local field. Then k is a non-discrete, totally disconnected, locally compact field in its v-topology. The valuation ring o(= p^o) and the ideals p_n of o, n ≥ l, are open, compact subgroups of the additive group of the field k, and they form a base of open neighbourhoods of 0 in k. Furthermore, o is the unique maximal compact subring of k.*

Proof. Let A be a complete set of representatives of T = o/p in o, containing 0 . Since T is a finite field, A is a finite set. Hence the set A =$\prod_{n=0}^{\infty} A_n$, A_n = A, is a compact set as a direct product of finite sets A_n , n ≥ O. Therefore,, o is compact in the v-topology. We already stated in that each p_n, n ≥ 0, is at the same time open and closed in k and that the p_n's gives us a base of open neighbourhoods of 0 in k so that k is a non-discrete, totally disconnected topological field. Since o is compact, k is locally compact, and since p_n is

closed in o, p_n is also compact. Let R be any compact subring of k. Then the compactness implies that the set $\{v(x)|x \in R\}$ is bounded below in the real field R. If x ∈ R, then $x^n \in$ R and v(x^n) = $n.v(x)$ for all n ≥ l. Hence, by the above remark, v(x) ≥ 0 that is, x ∈ o. This proves that R ⊆ 0 so that o is the unique maximal compact subring of the field k. QED

Proposition 10. *Let (k, v) be a local field.*

$$V = \{x \in k | x^{q-1} = 1\} \qquad A = V \cup \{0\} = \{x \in k | x^q = x\} \tag{47}$$

Then A is a complete set of representatives of T = o/p in o, containing 0; V is the set of all (q 1) roots of unity in k; and the canonical ring homomorphism o → T =o/p induces an isomorphism of multiplicative groups:

$$V \to T^{\times} \tag{48}$$

In particular, V is a cyclic group of order q 1.

Proof. Let A' = $\{w(x)|x \in o\}$. As w(x) = x mod p, each residue class of o mod p contains at least one element in A', and as $w(x)^q$ = w(x), A' is a subset of A. However, the number of elements x in k satisfying $x^q - x = 0$ is at most q, while the number of elements in T = o/p is q. Hence A = A' and A is a complete set of representatives of T = o/p in o. Obviously, 0= w(0) ∈ A. Since w(xy)= w(x)w(y), the other statements on V are clear.

Proposition 11. *Let (k, v) be a p-field of characteristic 0:*$\mathbb{Q} \subseteq k$. *Let e = v(p), where p = p . 1_k and let f = F_q , q = p^f, for the residue field T = o/p. Then (k, v) is a complete extension of the p-adic number field* $(\mathbb{Q}_p, v_p,)$ *and*

$$[k : Q_p] = ef < \infty \tag{49}$$

Furthermore, the valuation ring o of (k, v) is a free $\mathbb{Z}_p$*-module of rank ef =[k:* $\mathbb{Q}_p$ *].*

Proof. Let $\lambda = v|\mathbb{Q}$ Since (k,v) is a p-field and p = p.$l_k \neq 0$,

$$0 = \lambda(p) = v(p) < \infty \tag{50}$$

However, it is known that such a valuation λ on $\mathbb{Q}$ is equivalent to the p-adic valuation v_p, of $\mathbb{Q}$. Let k' denote the closure of $\mathbb{Q}$ in k. As (k, v) is complete, (k',v|k') is a completion of $(\mathbb{Q}, \lambda)$. It then follows from$\lambda \sim v_p$ that k' = $\mathbb{Q}_p$ and v$I\mathbb{Q}_p \sim v_p$. Hence (k, v) is a complete extension of $(\mathbb{Q}_p, v_p)$. Since v_p(p) = 1, y(p) = e, and v|$\mathbb{Q}_p$ = e(k|$\mathbb{Q}_p$)v_p , we obtain e(k|$\mathbb{Q}_p$) = e. On the other hand, T = $\mathbb{F}_q$, q = p^f, and $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$ f (k|$\mathbb{Q}_p$) = $f < \infty$. Therefore, [k :$\mathbb{Q}_p$] = ef and o is a free $\mathbb{Z}_p$-module of rank ef.

Proposition 12. *Let (k, v) be a p-field of characteristic p with $f = o/p = \mathbb{F}_g$ and let $(F_q((T)), v^T)$ denote the p-field of Laurent series in T. Then k contains F_q as a subfield and there exists an F_q isomorphism*

$$(k, v) \to (F_q((T)), v^T) \tag{51}$$

namely, an F_q-isomorphism $k \to F_g((T))$, which transfers the valuation v of k to the valuation $v^T of F_g((T))$.

Proof. Since k is a field of characteristic p, the set $A = \{x \in k | x^q = x\}$ is a subfield of k with q elements. Then $F_q = A \subseteq k$. Now, fix a prime element π of k, then for $A = F_q$ and $\pi_n = \pi^n, n \in \mathbb{Z}$. We then see that the map

$$\sum_n a_n \pi^n \to \sum_n a_n T^n, a_n \in F_q \tag{52}$$

defines an F_q -isomorphism (k,v): $\to (F_q((T)), v^T)$.
Taking account of the above propositions , we can get the following simple description of the family of all p-fields for a given prime number p, although the statement here is not as precise as in those propositions:

Theorem 21. *A field k is a p-field of characteristic 0 if and only if it is a finite extension of the p-adic number field $\mathbb{Q}_p$, and k is a p-field of characteristic p if and only if it is a finite extension of the Laurent series field $F_p((T))$.*

References

[Her05] Israel Nathan Herstein. *Noncommutative rings*. Number 15. Cambridge University Press, 2005.

[Isa08] I Martin Isaacs. *Finite group theory*, volume 92. American Mathematical Soc., 2008.

[Iwa86] Kenkichi Iwasawa. *Local class field theory*, volume 11. Oxford University Press, USA, 1986.

[Jac56] Nathan Jacobson. *Structure of rings*, volume 37. American Mathematical Soc., 1956.

[Jan73] Gerald J Janusz. *Algebraic number fields*. Elsevier, 1973.

[Lam06] Tsit-Yuen Lam. *Exercises in classical ring theory*. Springer Science & Business Media, 2006.

[Lam13] Tsi-Yuen Lam. *A first course in noncommutative rings*. Springer Science & Business Media, 2013.

[Row08] Louis Halle Rowen. *Graduate algebra: noncommutative view*, volume 91. American Mathematical Society, 2008.

[Ser13] Jean-Pierre Serre. *Local fields*, volume 67. Springer Science & Business Media, 2013.