COHOMOLOGY OF GROUPS

AND

Some Applications

by

Pranjal Rajkhowa

DEPARTMENT OF MATHEMATICS

Submitted in full-fillment of the requirement of
The Degree of Master of Philosophy

To

NORTH-EASTERN HILL UNIVERSITY

May 1980

A brief abstract of the dissertation "Co-homology of Groups and Some Applications" :

Chapter I deals with the definition of the nth. Cohomology Group and the interpretation of such groups of low order. We also prove some results and use them to give two applications.

In Chapter II we develop some theory of Centr Simple algebras and we define the Brauer Group of a fiel with a view to using these results in the next chapter.

Chapter III deals with the interpretation of the Brauer Group of a field in terms of Galois Cohomolog In this chapter,we first define Galois Cohomology and th prove some results to arrive at this interpretation.

Finally in Chapter IV we use this interpretab ion of the Brauer Group of a field to compute the Brauer Groups of certain specific fields,namely that of R, C and that of a finite field.

Certified that the above is an abstract of the study undertaken by Mr. Pranjal Rajkhowa,which forms the subject matter of his dissertation.

P. Jothilingam

P.Jothilingam.
Department of Mathematics
School of Physical Sciences
North-Eastern Hill University
Shillong.

phone :
Grams : NEHU

North-Eastern Hill University

LOWER LACHAUMIERE, SHILLONG - 793001

I certify that the dissertation entitled "Co-homology og Groups and Some Applications" submitted by Mr. Pranjal Rajkhowa in fullfillment of the requirements for the degree of Master of Philosophy is the outcome of a study undertaken by the candidate. I certify that sources from which ideas have been borrowed are duly referred to.

This dissertation may be placed before the examiners for evaluation and necessary formalities.

P. Jothilingam

P.Jothilingam.
Supervisor.

ACKNOWLEDGEMENTS

I wish to express my sincere thanks to Dr. P.Jothilingam , Head of the Department of Mathematics,North Eastern Hill University , who has guided me in the preparation of this dissertation and I thank him also for taking the pains of going through these pages.

I also thank Dr. M.B.Rege and Dr.S.S.Khare of the Department of Mathematics,NEHU,who have helped in many ways in the completion of this work.

Lastly I am very thankful to Mr. Danley D. Swer for his kind efforts in typing this manuscript for me.

Shillong, May 1980 .

(Pranjal Rajkhowa)

....

CONTENTS

CHAPTER 0

PRE-LIMINARY DEFINITIONS

***

This chapter is devoted to an explanation of certain pre-liminary definitions.

Ring - associative ring with identity.

Module - unitary left module.

Algebra - If R is a commutative ring, then by an R-algebra A we mean a ring A such that

i) A is an R-module

and ii) $\forall$ $\alpha \in R$ and $a, b \in A$, we have

$$\alpha(ab) = a(\alpha b) = (\alpha a)b .$$

Opposite Algebra - Let A be an R-algebra. Define a ring structure on A by the multiplication o such that aob = ba and addition as in the original structure. Denoting this new structure by A°, A° is called the opposite algebra of A.

Division ring - Ring with 1 in which every nonzero element has a multiplicative inverse.

Centre of a ring - The Centre of a ring R is the set

$$C = \{ r \in R : rs = sr \ \forall s \in R \} .$$

Noetherian Module - A left R-module satisfying any of the following equivalent conditions is called a left Noetherian R-module.

(a) Every strictly ascending chain of left R-submodules of M is finite.

(b) Every nonempty collection of left R-submodules of M has a maximal element.

(c) Every left R-submodule of M is finitely generated.

Similarly by replacing 'left' by 'right' in the

above definition we get the definition of a right Noetherian R-module.

Noetherian Ring - A ring R is called left (resp. right) Noetherian if it is left (resp. right) Noetherian as an R-module.

Artinian Module - If R is a ring, then an R-module M satisfying any of the two following equivalent conditions is called a left Artinian R-module:

(a) Every strictly descending chain of left R-submodules of M is finite.

(b) Every nonempty collection of left R-submodules of M has a minimal element.

Artinian Ring - A ring R is called left-Artinian if it is left Artinian as a left R-module.

Right Artinian rings and modules may be similarly defined.

For a commutative ring R, the notions of left and right Noetherian (resp. Artinian) rings or modules coincide.

Localization - A subset S of a ring R is called a multiplicative set if i) $1 \in S$ and ii) $a,b \in S \Rightarrow ab \in S$.

Let S be a multiplicative set in R. Consider the set $\{ r/s : r \in R, s \in S \}$.

We say that two such symbols r_1/s_1 and r_2/s_2

We write $m_1/s_1 \sim m_2/s_2$ if $\exists\ s \in S$ such that $s(s_1m_2 - s_2m_1) = 0$. Let M_S (or $S^{-1}M$) be the set of distinct equivalence classes and let $[m/s]$ denote the equivalence class of m/s.

We define an addition in M_S as

$$[m_1/s_1] + [m_2/s_2] = [s_2m_1 + s_1m_2/s_1s_2] .$$

and if $[r/s] \in R_S$, we define

$$[r/s]\cdot[m_1/s_1] = [rm_1/ss_1] .$$

With these two definitions, M_S becomes an R_S module. If $S = R - P$ for some prime ideal P of R, we denote M_S by M_P.

Algebraic Element - Let F be a field and K a field extension of F. An element $\alpha \in K$ is said to be algebraic over F if α satisfies some polynomial equation in one variable with coefficients in F.

Minimal Polynomial - $f(x)$ is said to be the minimal polynomial of an element $\alpha \in K$ over F if $f(x)$ is monic and of minimal degree such that $f(\alpha) = 0$.

Algebraic Extension - Let $F \subseteq K$ be fields. Then K is called an algebraic extension of F if every element of K is algebraic over F.

Normal Extension - An algebraic extension K of a field F is called a normal extension of F if each irreducible polynomial $f(x)$ over F having a root in K splits into linear factors over K.

Splitting Field - Let F be a field, and let $f(x) \in F[x]$. Let degree $f(x) = n \geq 1$. A field extension E of F is called a splitting field of $f(x)$ if (a) $f(x)$ can be factored into n linear factors over E, and (b) there does not exist any proper subfield E' of E containing F such that $f(x)$ can be factored into n linear factors over E'.

Separability - An irreducible polynomial $f(x) \in F[x]$ of degree n is said to be separable if it has n distinct roots in its splitting field; otherwise it is called inseparable.

If an element a of a field extension K of F is algebraic over F, then a is said to be separable (inseparable) over F if the minimal polynomial of a over F is separable (inseparable).

An algebraic extension K of a field F is said to be a separable extension if every element of K is separable over F; otherwise K is called an inseparable extension.

Simple Extension - A field extension K of F is called a simple extension of F if $K = F(a)$ for some $a \in F$.

F-automorphism - If K is a field extension of F then an automorphism σ of K is called an F-automorphism if $\sigma(x) = x \ \forall \ x \in F$.

Galois Group - Let $F \subseteq K$ be fields. The Galois group of K over F is the group of all F-automorphisms of K and is denoted by $\mathcal{G}_{K/F}$.

Fixed field - Let $\mathcal{G}$ be any group of automorphisms of a field K. Then the set $\{x \in K : \sigma(x) = x \; \forall \sigma \in \mathcal{G}\}$ is a subfield of K called the fixed field under $\mathcal{G}$.

Galois Extension - A finite extension K of a field F is called a Galois Extension of F if F is the fixed subfield of K under $\mathcal{G}_{K/F}$.

Norm and Trace - Let K be a finite normal extension of a field F of characterestic zero, and let $[K:F] = n$. Let $\sigma_1, \sigma_2, \sigma_3, \ldots\ldots, \sigma_n$ be all the F-automorphisms of K. For each $x \in K$, we define $N_{K/F}(x)$ and $T_{K/F}(x)$ called the norm and trace of x over F respectively as $N_{K/F}(x) = \prod_{i=1}^{n} \sigma_i(x)$ and $T_{K/F}(x) = \sum_{i=1}^{n} \sigma_i(x)$.

Exactness - Let M', M and M" be R-modules. A pair of homomorphisms $M' \xrightarrow{f} M \xrightarrow{g} M''$ is exact at M if Image f = kernel g. As a particular case, the sequence of R-modules and R-homomorphisms $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ is said to be exact if i) f is one-one, ii) g is onto, iii) kernel g = Image f.

Split Exact Sequence - Let $0 \to T \xrightarrow{\alpha} M \xrightarrow{\theta} N \to 0$ be an exact sequence of R-modules. Then the sequence is said to be split exact if $\exists$ an R-linear map $\eta : N \to M$ such that $\theta \circ \eta$ = Identity on N.

G-group - Let G be a group and let A be an abelian group. We say that the group G operates on A or G

..continued..

acts on A if $\exists$ a mapping $G \times A \to A$, $(g,a) \mapsto g \cdot a$ such that i) $(g_1 g_2)a = g_1(g_2 a)$ ii) $g(a+b) = ga + gb$ iii) $ea = a$ $\forall$ $g, g_1, g_2 \in G$ and $\forall$ $a, b \in A$. In this situation we say that A is a G-group.

We remark here that if G operates on A, the mapping $\rho_g : \begin{matrix} A \to A \\ a \mapsto g \cdot a \end{matrix}$ is an automorphism of A, and the mapping $\begin{matrix} G \to \text{Aut } A \\ g \mapsto \rho_g \end{matrix}$ is a group homomorphism.

Conversely, if G is a group and A an abelian group, and if $\eta : G \to \text{Aut } A$ such that $\eta(g) = \rho_g : \begin{matrix} A \to A \\ a \mapsto g \cdot a \end{matrix}$ is a homomorphism, then the group G operates on A.

<u>G-module</u> - Let $G = \{g_i : i \in I\}$ be any multiplicative group and let R be any commutative ring with 1.

Let R(G) denote the set of all formal sums $\sum_{i \in I} a_i g_i$ for $a_i \in R$ and $g_i \in G$ and where all but finitely many of the a_i's are zero.

Now if $x, y \in R(G)$, we may write $x = \sum_{i \in I} a_i g_i$ and $y = \sum_{i \in I} b_i g_i$.

We define an addition + , and a multiplication · in the elements of R(G) as follows :

$$x + y = \sum_{i \in I} a_i g_i + \sum_{i \in I} b_i g_i = \sum_{i \in I} (a_i + b_i) g_i$$

and $$x \cdot y = \left(\sum_{i \in I} a_i g_i \right) \left(\sum_{i \in I} b_i g_i \right) = \sum_{i \in I} \left(\sum_{g_j g_k = g_i} a_j b_k \right) g_i g_k$$

$\forall$ $x, y \in R(G)$.

Under these operations, the set R(G), becomes a ring called the group ring of G over R.

In particular if we take $R = \mathbb{Z}$, then we have the following :

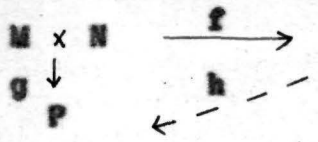
Definition - By a G-module A we mean a $Z(G)$ module A.

Remarks - (i) If A is a $Z(G)$ module, then A is an abelian group in particular. Since now, for any $g \in G$ we have $g = 1.g$ so $g \in \mathbb{Z}(G)$ and thus $g \cdot a \in A$. This gives an action of G on A. (ii) Conversely suppose a group G operates on an abelian group A. Any $x \in \mathbb{Z}(G)$ can be written as $x = \sum_{i \in I} n_i g_i$ where $n_i \in \mathbb{Z}$ and $g_i \in G$ and all but finitely many n_i's are zero. For $a \in A$ and $x \in \mathbb{Z}(G)$ define $x \cdot a = \sum_{i \in I} n_i (g_i a)$. Under this definition A becomes a $\mathbb{Z}(G)$-module i.e. a G-module.

G-homomorphism - Let G be any group and let A and B be G-modules. A homomorphism $A \xrightarrow{f} B$ is called a G-homomorphism if $f(gx) = g.f(x)$ $\forall$ $g \in G$ and $\forall$ $x \in A$.

Tensor Product of Modules - Let R be an associative ring with 1. Let M and N be respectively unitary right and left R-modules. Then the tensor product T of M and N is an abelian group together with a bi-additive map $f : M \times N \longrightarrow T$ satisfying $f(m\lambda, n) = f(m, \lambda n)$ $\forall$ $m \in M$, $n \in N$, $\lambda \in R$ and such that (i) $f(M \times N)$ generates T as an abelian group (ii) if P is any abelian group and if any bi-additive map $g : M \times N \longrightarrow P$ satisfying $g(m\lambda, n) = g(m, \lambda n)$ for $m \in M$, $n \in N$, $\lambda \in R$ is given, then $\exists$ a unique group homomorphism $h : T \longrightarrow P$ making the following

diagram commute (i.e. $hof = g$) :



Remarks : (1) The tensor product T of M and N is usually written $M \otimes_R N$, and it is unique upto group isomorphism.

(2) Let $\mathbb{Z}(M,N)$ be the free abelian group on the generators (m,n) where $m \in M$, $n \in N$. Let C be the submodule of $\mathbb{Z}(M,N)$ generated by the elements :
(i) $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$, (ii) $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$, (iii) $(m\lambda, n) - (m, \lambda n)$
$\forall\ m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ and $\lambda \in R$. Then $M \otimes_R N = \mathbb{Z}(M,N)/C$.

(3) The image under f of an element (m,n) is denoted by $m \otimes n$.

(4) When R is a commutative ring with 1, $M \otimes_R N$ can be given a unitary R-module structure in a canonical way.

Tensor Product of Algebras : Let R be a commutative ring with 1. Let A and B be R-algebras and let $f : R \to A$, $g : R \to B$ be the corresponding homomorphisms. Now $A \otimes_R B$ is in general an R-module. The mapping $h : (A \otimes_R B) \times (A \otimes_R B) \to A \otimes_R B$ such that $h((a_1 \otimes b_1), (a_2 \otimes b_2)) = a_1a_2 \otimes b_1b_2$ $\forall\ a_1, a_2 \in A$ and $b_1, b_2 \in B$, makes $A \otimes_R B$ into a ring. If $j : R \to A \otimes_R B$ is such that $j(x) = f(x) \otimes g(x)$ then under the ring homomorphism j, $A \otimes_R B$ becomes an R-algebra.

****

CHAPTER I

COHOMOLOGY OF GROUPS

****

In this chapter we define the nth Co-homology group and interpret lower dimensional groups of this kind, for instance, the zeroeth, the first and the second co-homology groups. In particular, we prove also that for a free group the second cohomology group is trivial. A few applications are also mentioned.

§ 1. Definitions of co-chains, cocycles and the nth. Co-homology group.

We assume that A is a G-group.

Homogeneous Co-chains - Let n be an integer $\geqslant 0$. Let $C^n_{hom}(G,A)$ denote the set of mappings $G^{n+1} \xrightarrow{F} A$ such that $F(gg_0, gg_1, \ldots, gg_n) = gF(g_0, g_1, \ldots, g_n)$ where g, g_i's $\in G$ $\forall$ i, $1 \leq i \leq n$. Any such F is called a homogeneous n-cochain, and the set of homogeneous cochains forms an abelian group under the addition of mappings and is denoted by $C^n_{hom}(G,A)$.

Non-homogeneous Co-chains - Let n be an integer $\geqslant 0$. Define $C^o_{N-hom}(G,A)$ to be the set of all elements of A. If $n \geqslant 1$, define a non-homogeneous n-cochain to be any mapping $f : G^n \longrightarrow A$. The set of all such mappings form an abelian group under the addition of mappings, and is denoted by $C^n_{N-hom}(G,A)$.

Proposition 1.1.1 - Let $n \geqslant 0$. There exists an iso-

morphism $\theta : C^n_{hom}(G,A) \longrightarrow C^n_{N\text{-}hom}(G,A)$.

Proof : Case I - Let $n \geq 1$.

Given $F \in C^n_{hom}(G,A)$, we define $\theta(F) = f$ where

$f(g_1,g_2,\ldots,g_n) = F(1,g_1,g_1g_2,\ldots,g_1g_2\ldots g_n)$ --(1)

In order to verify that θ is a group homomorphism let

$\theta(F_i) = f_i$, $i = 1,2$. Now $[\theta(F_1+F_2)](g_1,g_2,\ldots,g_n)$

$= (F_1+F_2)(1,g_1,g_1g_2,g_1g_2g_3,\ldots,g_1g_2\ldots g_n)$

$= F_1(1,g_1,g_1g_2,\ldots,g_1g_2g_3\ldots g_n) + F_2(1,g_1,g_1g_2,\ldots,g_1g_2\ldots g_n)$

$= f_1(g_1,g_2,\ldots,g_n) + f_2(g_1,g_2,\ldots,g_n)$

$= (f_1+f_2)(g_1,g_2,\ldots,g_n) = (\theta(F_1) + \theta(F_2))(g_1,g_2,\ldots,g_n)$

$\forall\ g_1,g_2,\ldots,g_n \in G$. This shows that

$\theta(F_1+F_2) = \theta(F_1) + \theta(F_2)$ $\forall\ F_1,F_2 \in C^n_{hom}(G,A)$ and

hence θ is a group homomorphism. Consider now

$\psi : C^n_{N\text{-}hom}(G,A) \longrightarrow C^n_{hom}(G,A)$ given by $\psi(f) = F$

where $F(g_0,\ldots,g_n) = g_0 f(g_0^{-1}g_1, g_1^{-1}g_2,\ldots,g_{n-1}^{-1}g_n)$ --(2)

Firstly $\psi(f)(gg_0,\ldots,gg_n) = gg_0 f(g_0^{-1}g^{-1}gg_1,\ldots,g_{n-1}^{-1}g^{-1}gg_n)$

$= g(g_0 f(g_0^{-1}g_1, g_1^{-1}g_2,\ldots,g_{n-1}^{-1}g_n))$

$= g(\psi(f)(g_0,g_1,\ldots,g_n))$

$= g\,\psi(f)(g_0,g_1,\ldots,g_n)$ $\forall\ g_i$'s $\in G$, $0 \leq i \leq n$.

Therefore $\psi(f) \in C^n_{hom}(G,A)$.

In order to show that ψ is a group homomorphism, let

$\psi(f_i) = F_i$ for $i = 1,2$. Then $\psi(f_1+f_2)(g_0,g_1,\ldots,g_n)$

$= g_0(f_1+f_2)(g_0^{-1}g_1, g_1^{-1}g_2,\ldots,g_{n-1}^{-1}g_n)$

$= g_0[f_1(g_0^{-1}g_1,\ldots,g_{n-1}^{-1}g_n) + f_2(g_0^{-1}g_1,\ldots,g_{n-1}^{-1}g_n)]$

$= g_0 f_1(g_0^{-1}g_1,\ldots,g_{n-1}^{-1}g_n) + g_0 f_2(g_0^{-1}g_1,\ldots,g_{n-1}^{-1}g_n)$

$= F_1(g_0,g_1,\ldots,g_n) + F_2(g_0,g_1,\ldots,g_n)$

$= \psi(f_1)(g_0,g_1,\ldots,g_n) + \psi(f_2)(g_0,g_1,\ldots,g_n)$

$\forall\ g_0,g_1,\ldots,g_n \in G$. Therefore ψ is a group homomorphism.

Next, $\psi \circ \theta$ = Identity. For $[(\psi\circ\theta)(F)](g_0,\ldots,g_n)$

$= \psi(\theta(F))(g_0,g_1,\ldots,g_n)$

$= g_0\ \theta(F)(g_0^{-1}g_1, g_1^{-1}g_2, \ldots, g_{n-1}^{-1}g_n)$ by --(2)

$= g_0 F(1, g_0^{-1}g_1, g_0^{-1}g_1g_1^{-1}g_2, \ldots)$ by --(1)

$= g_0 F(1, g_0^{-1}g_1, g_0^{-1}g_2, \ldots, g_0^{-1}g_n)$

$= F(g_0,g_1,g_2,\ldots,g_n)$, $\forall\ g_0,g_1,\ldots,g_n \in G$.

Hence $\psi \circ \theta$ = Identity on $C^n_{hom}(G,A)$.

Also $\theta \circ \psi$ = Identity. For $[(\theta\circ\psi)(f)](g_1,\ldots,g_n)$

$= \theta(\psi(f))(g_1,g_2,\ldots,g_n)$

$= \psi(f)(1,g_1,g_1g_2,\ldots,g_1g_2\ldots g_n)$ by --(1)

$= 1.f(1^{-1}g_1, g_1^{-1}g_1g_2, (g_1g_2)^{-1}g_1g_2g_3, \ldots)$ by --(2)

$= f(g_1,g_2,g_3,\ldots,g_n)$, $\forall\ g_1,g_2,\ldots,g_n \in G$.

Therefore $(\theta\circ\psi)(f) = f$ $\forall\ f \in {}_N\underline{C}^n_{hom}(G,A)$ and hence $\theta\circ\psi$ = Identity on $C^n_{N\text{-}hom}(G,A)$.

This shows that θ is an isomorphism and so $C^n_{hom}(G,A) \cong C^n_{N\text{-}hom}(G,A)$ for any $n \geq 1$.

<u>Case II</u> - Let $n = 0$.

Now $C^0_{hom}(G,A) = \{F : G' \to A : F(gg_0) = gF(g_0)\}$ and $C^0_{N\text{-}hom}(G,A) = A$ by definition. Consider $\theta : C^0_{hom}(G,A) \to A$ given by $\theta(F) = F(1)$. This is a group homomorphism. Let $\psi : A \to C^0_{hom}(G,A)$ be defined as $\psi(a) = \tilde{a}$ where $\tilde{a}(g_0) = g_0a$ for any $g_0 \in G$. Notice that $\tilde{a}(gg_0) = gg_0a = g\,\tilde{a}(g_0)$, so that $\tilde{a}$ is homogeneous. Now $\psi\circ\theta(F) = \psi(\theta(F)) = \psi(F(1)) = \widetilde{F(1)}$.

But $\widetilde{F(1)}(g_o) = g_o F(1)$ by definition,

$= F(g_o)$, because F is homogeneous. So $F = \widetilde{F(1)}$. Thus $(\psi \circ \theta)(F) = F$, $\forall F \in C^o_{hom}(G,A)$. Also $(\theta \circ \psi)(a) = \theta(\psi(a)) = \theta(\tilde{a}) = \tilde{a}(1) = 1.a = a$ so that $\theta \circ \psi(a) = a$, $\forall a \in A$. Hence θ is an isomorphism i.e. $C^o_{hom}(G,A) \simeq C^o_{N-hom}(G,A) = A$. #

<u>Boundary Operators</u> - Let $n \geq 0$ (integer). Define a mapping $\partial_n : C^n_{hom}(G,A) \longrightarrow C^{n+1}_{hom}(G,A)$ given by $(\partial_n F)(g_o,g_1,\ldots,g_n,g_{n+1}) = \sum_{i=0}^{n+1} (-1)^i F(g_o,g_1,\ldots,\hat{g}_i,g_{i+1},\ldots,g_{n+1})$ where $F \in C^n_{hom}(G,A)$ and g_i's $\in G$, $\forall i$, $0 \leq i \leq n+1$ ∂_n is called the <u>nth boundary operator</u>.

<u>Proposition 1.1.2</u> - (a) ∂_n is a group homomorphism.

(b) $\partial_{n+1} \circ \partial_n = 0$ for any $n \geq 0$.

<u>Proof</u> - (a)

$$\partial_n(F+G)(g_o,g_1,\ldots,g_{n+1})$$
$$= \sum_{i=0}^{n+1} (-1)^i (F+G)(g_o,g_1,\ldots,\hat{g}_i,\ldots,g_{n+1})$$
$$= \sum_{i=0}^{n+1} (-1)^i F(g_o,g_1,\ldots,\hat{g}_i,\ldots,g_n,g_{n+1})$$
$$+ \sum_{i=0}^{n+1} (-1)^i G(g_o,g_1,\ldots,\hat{g}_i,\ldots,g_n,g_{n+1})$$
$$= \partial_n F(g_o,g_1,\ldots,g_{n+1}) + \partial_n G(g_o,g_1,\ldots,g_{n+1})$$

$\forall g_i$'s $\in G$, $0 \leq i \leq n+1 \Rightarrow \partial_n(F+G) = \partial_n(F) + \partial_n(G)$

$\forall F,G \in C^n_{hom}(G,A)$

(b)

$$(\partial_{n+1}(\partial_n F))(g_o,\ldots,g_{n+2})$$
$$= \sum_{i=o}^{n+2} (-1)^i \partial_n F(g_o,\ldots,\hat{g}_i,\ldots,g_{n+2})$$

$$= \sum_{i=0}^{n+2} (-1)^i \sum_{\substack{j=0 \\ j<i}}^{n+2} (-1)^j F(g_0,\ldots,\hat{g}_j,\ldots,\hat{g}_i,\ldots,g_{n+2})$$
$$+ \sum_{i=0}^{n+2} (-1)^i \sum_{\substack{j=0 \\ j>i}}^{n+2} (-1)^{j-1} F(g_0,\ldots,\hat{g}_i,\ldots,\hat{g}_j,\ldots,g_{n+2})$$
$$= 0 \qquad \#$$

<u>Remark 1.1.1</u> - For $n \geq 1$, consider the following commutative diagram : $C^n_{hom}(G,A) \xrightarrow{\partial_n = \partial} C^{n+1}_{hom}(G,A)$

$$\downarrow\wr \qquad\qquad \downarrow\wr$$
$$C^n_{N\text{-}hom}(G,A) \xrightarrow{\partial} C^{n+1}_{N\text{-}hom}(G,A) ,$$

Let $f \in C^n_{N\text{-}hom}(G,A)$ be identified with $F \in C^n_{hom}(G,A)$ as mentioned earlier. Under this identification, let $\partial_n f$ be identified with $\partial_n F$ (For convenience we will write ∂ for ∂_n.)

<u>Proposition 1.1.3</u> - For every $(g_1,\ldots,g_{n+1}) \in G^{n+1}$,

$$(\partial f)(g_1,g_2,\ldots,g_{n+1}) = g_1 f(g_2,\ldots,g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1,g_2,\ldots,g_{i-1},g_i g_{i+1},$$
$$g_{i+2},\ldots,g_{n+1}) + (-1)^{n+1} f(g_1,g_2,\ldots,g_n)$$

<u>Proof</u> :- R.H.S. $= g_1 F(1,g_2,g_2g_3,\ldots,g_2g_3\cdots g_{n+1})$
$$+ \sum_{i=1}^{n} (-1)^i F(1,g_1,g_1g_2,\ldots,g_1g_2\cdots g_{i-1},$$
$$\overbrace{g_1g_2\cdots g_{i-1}g_i}^{},\ldots,g_1g_2\cdots g_{n+1})$$
$$+ (-1)^{n+1} F(1,g_1,g_1g_2,\ldots,g_1g_2\cdots g_n)$$
$$= F(g_1,g_1g_2,\ldots,g_1g_2\cdots g_{n+1})$$
$$+ \sum_{i=1}^{n} (-1)^i F(1,g_1,g_1g_2,\ldots,\overbrace{g_1g_2\cdots g_{i-1}g_i}^{},\ldots,g_1g_2\cdots g_{n+1})$$
$$+ (-1)^{n+1} F(1,g_1,g_1g_2,\ldots,g_1g_2\cdots g_n) .$$

$$\text{L.H.S.} = (\partial F)(1, g_1, g_1g_2, \ldots, g_1g_2\cdots g_{n+1})$$

$$= \sum_{i=0}^{n+1} (-1)^i F(1, g_1, g_1g_2, \ldots, g_1g_2\cdots g_{n+1})$$

$$= F(g_1, g_1g_2, g_1g_2g_3, \ldots, g_1g_2\cdots g_{n+1})$$

$$+ \sum_{i=1}^{n} (-1)^i F(1, g_1, g_1g_2, \ldots, g_1g_2\cdots g_{n+1})$$

$$+ (-1)^{n+1} F(1, g_1, g_1g_2, \ldots, g_1g_2\cdots g_{n+1}) .$$

Hence the proposition. #

Notice that the above diagram commutes.

Remark 1.1.2 : Consider the following commutative diagram:

$$\begin{array}{ccc} C^0_{hom}(G,A) & \xrightarrow{\partial_0 = \partial} & C^1_{hom}(G,A) \\ \downarrow\wr & & \downarrow\wr \\ C^0_{N\text{-}hom}(G,A) & \longrightarrow & C^1_{N\text{-}hom}(G,A) \end{array}$$

As before, let f be identified with F and f be identified with ∂F under this identification.

Now $\partial F \in C^1_{hom}(G,A)$ so that $F : G^2 \to A$ and $\partial f \in C^1_{N\text{-}hom}(G,A)$ so that $\partial f : G \to A$. The element in $C^1_{N\text{-}hom}(G,A)$ corresponding to ∂F in $C^1_{hom}(G,A)$ is some $\tilde{f} : G \to A$. Let $\partial F = \tilde{F}$. Now $\tilde{f}(g) = \tilde{F}(1,g)$

$$= (\partial F)(1,g) = F(g) - F(1)$$

$$= gF(1) - F(1) = ga - a, \quad \text{where } F(1) = a.$$

Thus for $n = 0$, $\partial f(g) = ga - a$, for every $g \in G$. #

Remark 1.1.3 : Let $Z^n(G,A)$ denote the kernel of the homomorphism $\partial_n : C^n_{hom}(G,A) \to C^{n+1}_{hom}(G,A)$, $n \geq 0$ (integer). Let $B^n(G,A)$ denote the image of $\partial_{n-1} : C^{n-1}_{hom}(G,A) \to C^n_{hom}(G,A)$, $\forall\ n \geq 1$. For $n = 0$, define $B^0(G,A) = (o)$.

Notice that $Z^n(G,A)$ is isomorphic to the kernel of the homomorphism $\partial'_n : C^n_{N\text{-}hom}(G,A) \to C^{n+1}_{N\text{-}hom}(G,A)$ and

that $B^n(G,A)$ is isomorphic to the image of $\partial'_{n-1}: C^{n-1}_{N-hom}(G,A) \to C^n_{N-hom}(G,A)$, $n \geq 1$. Since $\partial_n \circ \partial_{n-1} = 0$, we have, $B^n(G,A) \subset Z^n(G,A)$, $\forall\, n \geq 0$.

Definition 1.1.1 : Any element of $Z^n(G,A)$ is called an n-cocycle and any element of $B^n(G,A)$ is called an n-coboundary. The group $Z^n(G,A)/B^n(G,A)$ is called the nth. Cohomology group of G with coefficients in A, and is denoted by $H^n(G,A)$ for any $n \geq 0$.

====

§2. Interpretation of H°, H^1, H^2 - Group Extensions.

In this section we interpret the zeroeth, the first and the second Cohomology groups. We assume as before that A is a G-group.

Let us define A^G to be the set $\{ a \in A : ga = a \ \forall g \in G \}$.

Proposition 1.2.1 : $H^\circ(G,A) = A^G$.

Proof : Now $H^\circ(G,A) = Z^\circ(G,A)/B^\circ(G,A) = Z^\circ(G,A)$.
Also $f \in Z^\circ(G,A) \Rightarrow \partial_0 f = 0 \Leftrightarrow \partial_0 f(g) = 0 \ \forall g \in G$. But $\partial_0 f(g) = ga - a$ by Remark 1.1.2. So $\partial_0 f(g) = 0 \ \forall g \in G \Leftrightarrow ga - a = 0 \ \forall g \in G \Leftrightarrow ga = a \ \forall g \in G$. Thus $H^\circ(G,A) = Z^\circ(G,A) = \{ f \in C^\circ_{N-hom}(G,A) : \partial_0 f = 0 \}$ $= \{ f \in C^\circ_{N-hom}(G,A) : \partial_0 f(g) = 0 \ \forall g \in G \} = \{ a \in A : ga = a \ \forall g \in G \} = A^G$.
Notice that A^G is a subgroup of A. #

Description of $H^1(G,A)$

Definition 1.3.1 : A mapping $f : G \to A$ is called a **crossed homomorphism** if $f(gh) = gf(h) + f(g)$ $\forall\ g,h \in G$.

If G acts trivially on A then any homomorphism on G is a crossed homomorphism.

Definition 1.3.2 : A mapping $f : G \to A$ is called a **principal homomorphism** if $\exists\ a \in A$ such that $f(g) = ga - a$ $\forall\ g \in G$.

Remark 1.3.1 : The zero mapping $G \to A$ is a principal homomorphism. Also if f is a principal homomorphism, then $\exists\ a \in A$ such that $f(gh) = gha - a$ $\forall\ g,h \in G$.

Now $gf(h) + f(g) = g\{ha - a\} + \{ga - a\}$

$= gha - a = f(gh)$.

Thus $f(gh) = gf(h) + f(g)$, so that any principal homomorphism is a crossed homomorphism. In fact the set of principal homomorphisms of G is a subgroup of the set of crossed homomorphisms of G. The latter is of course, an abelian group.

Proposition 1.3.2 : $H^1(G,A) = \dfrac{\text{group of crossed homomorphisms of } G}{\text{group of principal homomorphisms of } G}$

Proof : We have, $H^1(G,A) = Z^1(G,A)/B^1(G,A)$.

By definition, $f \in Z^1(G,A) \Leftrightarrow \partial_1 f = 0$. Now $\partial_1 f$ is a mapping from $G^2 \to A$, and $\partial_1 f(g,h) = gf(h) - f(gh) + f(g)$ by Remark 1.1.1 . Therefore $\partial_1 f(g,h) = 0 \Leftrightarrow f(gh) = gf(h) + f(g)$. Thus an N-homogeneous 1-cocycle corresponds to a crossed homomorphism.

Consider now $f \in B^1(G,A)$ that is $f \in$ the image of

$\partial_0 : C^0_{N\text{-hom}}(G,A) \to C^1_{N\text{-hom}}(G,A)$. Let $f = \partial_0 \tilde{f}$ where $\tilde{f} \in C^0_{N\text{-hom}}(G,A)$. So $f(g) = \partial_0 \tilde{f}(g) = ga - a$ for some $a \in A$ and $\forall\ g \in G$. Therefore $f \in B^1(G,A)$. Thus an N-homogeneous 1-coboundary corresponds to a principal homomorphism.

Hence $H^1(G,A) = \dfrac{Z^1(G,A)}{B^1(G,A)} = \dfrac{\text{group of crossed homomorphisms of } G}{\text{group of principal homomorphisms of } G}$.

#

Remark 1.3.2 : If the action of G on A is trivial, then $H^1(G,A) = \text{Hom}(G,A)$.

Description of $H^2(G,A)$

Assume that A is an abelian group and that the group G operates on A.

An extension of G by A is an exact sequence $1 \to A \xrightarrow{\alpha} \bar{G} \xrightarrow{\beta} G \to 1$, where $\bar{G}$ is any group, such that the following holds : if $\sigma \in G$ is given, and if $g \in \bar{G}$ is any particular pre-image of σ , then the map $\theta_g : A \to A$ such that $\theta_g(a) = gag^{-1}$, (an automorphism of A which depends only on σ and not on the particular choice of pre-image.) In this way we get an action of G on A. We demand that this action should coincide with the given action of G on A.

Remark 1.3.3 : If the action of G on A is trivial, then $1 \to A \xrightarrow{i} G \times A \xrightarrow{p} G \to 1$ with $i(a) = (1,a)$ and $p(g,a) = g$ is a group extension.

Again if we take $A = n\mathbb{Z}$, $G = \mathbb{Z}/n\mathbb{Z}$ and $\bar{G} = \mathbb{Z}$, then with the trivial action, $0 \to n\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$ is a group extension.

Equivalence of Extensions :

Let $1 \longrightarrow A \longrightarrow \overline{G}_1 \longrightarrow G \longrightarrow 1$ ---(1)

and $1 \longrightarrow A \longrightarrow \overline{G}_2 \longrightarrow G \longrightarrow 1$ ---(2)

be two extensions of G by A. We say that they are equivalent if $\exists$ an isomorphism $\theta : \overline{G}_1 \longrightarrow \overline{G}_2$ such that the following diagram commutes :

$$\begin{array}{ccccccc} 1 & \longrightarrow & A & \longrightarrow & \overline{G}_1 & \longrightarrow & G \longrightarrow 1 \\ & & \downarrow id & & \downarrow \theta & & \downarrow id \\ 1 & \longrightarrow & A & \longrightarrow & \overline{G}_2 & \longrightarrow & G \longrightarrow 1 \end{array}$$

It is easy to notice that the equivalence of extensions defines an equivalence relation in the set of all extensions of G by A.

We now prove the following

Proposition 1.3.3 : There exists a bijective correspondence between two co-homology classes of G in A and equivalence classes of extensions of G by A. (By co-homology classes we mean equivalence classes of cocycles).

Proof : Let $1 \longrightarrow A \longrightarrow \overline{G} \xrightarrow{\theta} G \longrightarrow 1$ be an extension of G by A. Let $\{u_\sigma\}_{\sigma \in G}$ be a section of the map $\theta : \overline{G} \longrightarrow G$. Thus under θ, $u_\sigma \mapsto \sigma$, $u_\tau \mapsto \tau$ and $u_\sigma u_\tau \longmapsto \sigma\tau$. But then $u_{\sigma\tau} \longmapsto \sigma\tau$. Therefore $\theta(u_\sigma u_\tau (u_{\sigma\tau})^{-1}) = \sigma\tau\tau^{-1}\sigma^{-1} = 1$

$\Rightarrow u_\sigma u_\tau (u_{\sigma\tau})^{-1} \in \ker\theta = A$. Say $u_\sigma u_\tau (u_{\sigma\tau})^{-1} = a_{\sigma,\tau} \in A$ for some element, denoted by $a_{\sigma,\tau}$, of A.

$\Rightarrow u_\sigma u_\tau = a_{\sigma,\tau}\, u_{\sigma\tau}$ ---(1). Thus for every pair $\sigma, \tau \in G$, $\exists\ a_{\sigma,\tau} \in A$ such that (1) holds.

In order to show that $a_{\sigma,\tau}$ is a 2-cocycle in the multiplicative notation, let $\sigma, \tau, \rho \in G$. Then $(u_\sigma u_\tau)u_\rho = u_\sigma(u_\tau u_\rho)$ ---(2). The L.H.S. of (2) $= a_{\sigma,\tau}\, u_{\sigma\tau}\, u_\rho = a_{\sigma,\tau}\, a_{\sigma\tau,\rho}\, u_{\sigma\tau\rho}$,

and the R.H.S. of (2) = $u_\sigma(a_{\tau,\rho}\, u_{\tau\rho})$ ---(3). Notice that for any $a \in A$, $u_\sigma a\, u_\sigma^{-1}$ coincides with the given action of G by A. Denoting the given action by a^σ, we can write $u_\sigma a\, u_\sigma^{-1} = a^\sigma$ i.e. $u_\sigma a = a^\sigma u_\sigma$. Therefore the R.H.S. of (2) = $a^\sigma_{\tau,\rho}\, u_\sigma u_{\tau\rho} = a^\sigma_{\tau,\rho}\, a_{\sigma,\tau\rho}\, u_{\sigma\tau\rho}$. Hence because of the equality in (2), we must have $a_{\sigma,\tau} a_{\sigma\tau,\rho}\, u_{\sigma\tau\rho} = a^\sigma_{\tau,\rho}\, a_{\sigma,\tau\rho}\, u_{\sigma\tau\rho}$ $\Rightarrow$ $a_{\sigma,\tau}\, a_{\sigma\tau,\rho} = a^\sigma_{\tau,\rho}\, a_{\sigma,\tau\rho}$ $\Rightarrow a^\sigma_{\tau,\rho}\, a_{\sigma,\tau\rho}\, a^{-1}_{\sigma,\tau}\, a^{-1}_{\sigma\tau,\rho} = 1$. (We shall call this the cocycle condition). Thus in the multiplicative notation, $a_{\sigma,\tau}$ is a 2-cocycle. The 2-cocycle $a_{\sigma,\tau}$ defines a cohomology class, i.e. an equivalence class of 2-cocycles.

Suppose now
$$\begin{array}{ccccccc} 1 & \longrightarrow & A & \longrightarrow & \bar{G}_1 & \longrightarrow & G \longrightarrow 1 \\ & & \| id & & \downarrow f & & \| id \end{array}$$
and
$$1 \longrightarrow A \longrightarrow \bar{G}_2 \longrightarrow G \longrightarrow 1$$
are two equivalent extensions. We will prove that they give rise to the same co-homology class.

Let $\{u_\sigma\}_{\sigma\in G}$ and $\{v_\sigma\}_{\sigma\in G}$ be chosen sections of the maps $\bar{G}_1 \longrightarrow G$ and $\bar{G}_2 \longrightarrow G$ respectively. For convenience, we identify $\bar{G}_1$ with $\bar{G}_2$ through the isomorphism $f : \bar{G}_1 \to \bar{G}_2$. Under this identification, $\sigma \in G$ has two pre-images u_σ and v_σ, and so they differ by an element of A, say c_σ. i.e. $u_\sigma = c_\sigma v_\sigma$ $\forall\, \sigma \in G$. (Here we are writing u_σ instead of $f(u_\sigma)$ by the identification). Thus $u_\sigma u_\tau = (c_\sigma v_\sigma)(c_\tau v_\tau) = c_\sigma c_\tau^\sigma v_\sigma v_\tau$ $= c_\sigma c_\tau^\sigma b_{\sigma,\tau}\, v_{\sigma\tau}$ where $b_{\sigma,\tau}$ is the 2cocycle associated with the section $\bar{G}_2 \longrightarrow G$. Also $u_\sigma u_\tau = a_{\sigma,\tau}\, u_{\sigma\tau}$, where $a_{\sigma,\tau}$ is the 2-cocycle associated with the section $\bar{G}_1 \longrightarrow G$.

Thus $u_\sigma u_\tau = a_{\sigma,\tau}\, u_{\sigma\tau} = a_{\sigma,\tau}\, c_{\sigma\tau}\, v_{\sigma\tau}$. Therefore $a_{\sigma,\tau}\, c_{\sigma\tau} =$

$c_\sigma c_\tau^\sigma b_{\sigma,\tau}$, so that $a_{\sigma,\tau} = \frac{c_\sigma c_\tau^\sigma}{c_{\sigma\tau}} b_{\sigma,\tau}$. Notice that $\frac{c_\sigma c_\tau^\sigma}{c_{\sigma\tau}}$ is a non-homogeneous 2-coboundary. Thus $a_{\sigma,\tau}$ and $b_{\sigma,\tau}$ belong to the same co-homology class i.e. they are co-homologous. Therefore $\{a_{\sigma,\tau}\}$ and $\{b_{\sigma,\tau}\}$ define the same 2-cohomology class of G in A. (The braces denoting co-homology classes). We have thus constructed a mapping θ : $\{$Equivalence classes of Extensions$\}$ $\longrightarrow$ $\{$Cohomology classes$\}$ as the class of the extension $1 \to A \to \bar{G} \to G \to 1$ being mapped into $\{a_{\sigma,\tau}\}$.

We construct now the map

η : $\{$Cohomology classes$\}$ $\to$ $\{$Equivalence classes of Extensions$\}$

inverse to θ as follows : Let $a_{\sigma,\tau}$ be a 2-cocycle representing a given 2-cohomology class. Let $\bar{G}$ be the set of pairs (a,σ), $a \in A$ and $\sigma \in G$. We will make $\bar{G}$ into a group as follows : Define a multiplication $\cdot$ on elements of $\bar{G}$ as $(a,\sigma)\cdot(b,\tau) = (ab^\sigma a_{\sigma,\tau}, \sigma\tau)$. We now show that $\bar{G}$ is a group with this multiplication.

Associativity : We have $[(a,\sigma)(b,\tau)](c,\rho) = (ab^\sigma a_{\sigma,\tau}, \sigma\tau)(c,\rho) = (ab^\sigma a_{\sigma,\tau} c^{\sigma\tau} a_{\sigma\tau,\rho}, \sigma\tau\rho)$ and $(a,\sigma)[(b,\tau)(c,\rho)] = (a,\sigma)[bc^\tau a_{\tau,\rho}, \tau\rho] = (ab^\sigma c^{\sigma\tau} a_{\tau,\rho}^\sigma a_{\sigma,\tau\rho}, \sigma\tau\rho)$. Since by the cocycle condition $a_{\sigma,\tau} a_{\sigma\tau,\rho} = a_{\tau,\rho}^\sigma a_{\sigma,\tau\rho}$, we get the required associativity.

Identity : The left-identity e of $\bar{G}$ is $(a_{1,1}^{-1}, 1)$, for $(a_{1,1}^{-1}, 1)(a,\sigma) = (a_{1,1}^{-1} a\, a_{1,\sigma}, \sigma)$ ---(1) by

definition. Consider now the cocycle condition $a_{\sigma,\tau}\, a_{\sigma\tau,\rho} = a_{\tau,\rho}^{\sigma}\, a_{\sigma,\tau\rho}$. Putting $\sigma = \tau = 1$, we get $a_{1,1}a_{1,\rho} = a_{1,\rho}\, a_{1,\rho}$ i.e. $a_{1,\rho} = a_{1,1}$ $\forall$ ρ so that in particular, $a_{1,\sigma} = a_{1,1}$. Thus $(a_{1,1}^{-1},1)(a,\sigma) = (a_{1,1}^{-1} a\, a_{1,\sigma}, \sigma) = (a,\sigma)$.

Inverse : The inverse of (a,σ) is $\left((a^{-1})^{\sigma^{-1}}\, a_{1,1}^{-1}\, a_{\sigma^{-1},\sigma}^{-1}\, ,\ \sigma^{-1}\right)$, for $\left((a^{-1})^{\sigma^{-1}}\, a_{1,1}^{-1} a_{\sigma^{-1},\sigma}^{-1}\, ,\ \sigma^{-1}\right)(a,\sigma)$ $= \left((a^{-1})^{\sigma^{-1}}\, a_{1,1}^{-1}\, a_{\sigma^{-1},\sigma}^{-1}\, a^{\sigma^{-1}}\, a_{\sigma^{-1},\sigma}\, ,1\right) = (a_{1,1}^{-1}\, ,1) = e$.

Thus $\bar{G}$ is a group.

Consider now the following surjective homomorphism $\lambda : \bar{G} \to G$ such that $\lambda(a,\sigma) = \sigma$. The kernel consists of elements $(a,1)$, $a \in A$. We now define a mapping $\psi : A \to$ kernel λ such that $a \mapsto (aa_{1,1}^{-1},1)$. This is a group homomorphism since $\psi(a)\,\psi(b) = (aa_{1,1}^{-1},1)(ba_{1,1}^{-1},1) = (aa_{1,1}^{-1}ba_{1,1}^{-1}a_{1,1},1) = (aba_{1,1}^{-1},1) = \psi(ab)$, for any $a,b \in A$. Next ψ is one one, for $\psi(a) = e$ $\Rightarrow (aa_{1,1}^{-1},1) = e \Rightarrow (aa_{1,1}^{-1},1) = (a_{1,1}^{-1},1) \Rightarrow a = 1$, the identity of A. Again ψ is surjective, since, for any $a \in A$, we can write $(a,1)$ as $(aa_{1,1}a_{1,1}^{-1},1)$ which is the image of $aa_{1,1}$ under ψ . We, therefore, get an exact sequence $1 \to A \xrightarrow{\psi} \bar{G} \xrightarrow{\lambda} G \to 1$. We now check that the action of G on A given by the above exact sequence is the same as the given action of G on A. Let $u_\sigma = (1,\sigma)$. Then $\{u_\sigma\}_{\sigma \in G}$ is a section of $\bar{G} \to G$. We can write (a,σ) as $\bar{a}u_\sigma$ where $\bar{a} = (aa_{1,1}^{-1},1)$ because $(aa_{1,1}^{-1},1)(1,\sigma) = (aa_{1,1}^{-1}a_{1,\sigma},\sigma) = (a,\sigma)$ since

$a_{1,\sigma} = a_{1,1}$ by the cocycle condition. Identify A with the subgroup $\bar{A}$ of $\bar{G}$ through the injection $a \longmapsto (aa_{1,1}^{-1}, 1) = \bar{a}$. Then the given action of G on A can be transported to an action of G on $\bar{A}$ as follows : Define $(\bar{a})^{\sigma} = \overline{a^{\sigma}}$. Now $u_{\sigma}\bar{a} = (1,\sigma)(aa_{1,1}^{-1}, 1) = \left(a^{\sigma}(a_{1,1})^{\sigma^{-1}} a_{\sigma,1}, \sigma\right)$. Also $(\bar{a})^{\sigma} u_{\sigma} = \overline{a^{\sigma}} u_{\sigma} = (a^{\sigma} a_{1,1}^{-1}, 1)(1,\sigma)$ $= (a^{\sigma} a_{1,1} a_{1,\sigma}, \sigma)$. Considering the cocycle condition, i.e. $a_{\sigma,\tau} a_{\sigma\tau,\rho} = a_{\tau,\rho}^{\sigma} a_{\sigma,\tau\rho}$ and putting $\tau = \rho = 1$, one gets $a_{\sigma,1} a_{\sigma,1} = a_{1,1} a_{\sigma,1}^{\sigma}$ which gives $a_{\sigma,1}(a_{1,1}^{\sigma})^{-1} =$ Identity. Also $a_{1,\sigma} = a_{1,1}$ so that $a_{1,1}^{-1} a_{1,\sigma} =$ Identity. Thus $u_{\sigma}\bar{a} = (\bar{a})^{\sigma} u_{\sigma}$. This shows that $1 \to A \to \bar{G} \to G \to 1$ is an extension.

We now show that the inverse map η is well-defined. For this, let $\{a_{\sigma,\tau}\}$ and $\{b_{\sigma,\tau}\}$ be cohomologous. Then $\exists$ $c_{\sigma} \in A$ $\forall$ $\sigma \in G$ such that $a_{\sigma,\tau} = \dfrac{c_{\sigma} c_{\tau}^{\sigma}}{c_{\sigma\tau}} b_{\sigma,\tau}$ ---(2). Let $1 \to A \to \bar{G}_1 \to G \to 1$ correspond to $\{a_{\sigma,\tau}\}$ and let $1 \to A \to \bar{G}_2 \to G \to 1$ correspond to $\{b_{\sigma,\tau}\}$. We are to construct an isomorphism $\lambda : \bar{G}_1 \to \bar{G}_2$ such that the diagram

$$\begin{array}{ccccccc} 1 & \to & A & \to & \bar{G}_1 & \to & G \to 1 \\ & & \| id & & \downarrow \lambda & & \| id \\ 1 & \to & A & \to & \bar{G}_2 & \to & G \to 1 \end{array}$$

commutes. Define $\lambda : \bar{G}_1 \to \bar{G}_2$ such that $\lambda(a,\sigma) = (ac_{\sigma},\sigma)$. λ is a group homomorphism for $\lambda(a,\sigma)(b,\tau) = \lambda(ab^{\sigma} a_{\sigma,\tau}, \sigma\tau)$ $= (ab^{\sigma} a_{\sigma,\tau} c_{\sigma\tau}, \sigma\tau)$. Also $(ac_{\sigma}, c)(bc_{\tau}, \tau) = (ac_{\sigma} b^{\sigma} c_{\tau}^{\sigma} b_{\sigma,\tau}, \sigma\tau)$ i.e. $\lambda(a,\sigma)\lambda(b,\tau) = ac_{\sigma} b^{\sigma} c_{\tau}^{\sigma} b_{\sigma,\tau}, \sigma\tau)$. Using (2) one gets that λ is a homomorphism. Again if we define $\mu : \bar{G}_2 \to \bar{G}_1$ such that $\mu(a,\sigma) = (ac_{\sigma}^{-1}, \sigma)$ then $\mu \circ \lambda =$

Identity and $\lambda \circ \mu$ = Identity. Therefore λ is an isomorphism.

The commutativity of the following diagram is a routine verification

$$\begin{array}{ccccccc} 1 & \to & A & \to & \bar{G}_1 & \to & G & \to & 1 \\ & & \| id & & \downarrow \lambda & & \| id & & \\ 1 & \to & A & \to & \bar{G}_2 & \to & G & \to & 1 \end{array}$$

Hence the associated extensions are equivalent, and the mapping η is well defined.

For the proof of the proposition to be complete, we need to show now that $\theta \circ \eta$ = Identity and $\eta \circ \theta$ = Identity. In order to show that $\theta \circ \eta$ is identity, let $\{a_{\sigma,\tau}\}$ be given, and let $1 \to A \to \bar{G} \to G \to 1$ be the associated extension. We choose the section $\{u_\sigma\}_{\sigma \in G}$, where $u_\sigma = (1,\sigma)$, for the map $\bar{G} \to G$. We compute the associated cocycle : Now $u_\sigma u_\tau = (1,\sigma)(1,\tau) = (a_{\sigma,\tau}, \sigma\tau)$ $= \bar{a}_{\sigma,\tau}\, u_{\sigma\tau}$ (by definition), which is the associated cocycle we started with. Hence $\theta \circ \eta$ = Identity. In order to show that $\eta \circ \theta$ = Identity, consider an extension $1 \to A \to \bar{G} \to G \to 1$. Let $\{u_\sigma\}_{\sigma \in G}$ be a chosen section and let $a_{\sigma,\tau}$ be the associated 2-cocycle. Let $\eta(a_{\sigma,\tau}) = 1 \to A \to \hat{G} \to G \to 1$. We are to construct an isomorphism $h : \hat{G} \to \bar{G}$ such that the diagram

$$\begin{array}{ccccccc} 1 & \to & A & \to & \hat{G} & \to & G & \to & 1 \\ & & \| id & & \downarrow h & & \| id & & \\ 1 & \to & A & \to & \bar{G} & \to & G & \to & 1 \end{array} \qquad \text{---(3)}$$

is commutative. Define $h : \hat{G} \to \bar{G}$ as $h(a,\sigma) = a \cdot u_\sigma$

Now $h((a,\sigma)(b,\tau)) = h(ab^{\sigma} a_{\sigma,\tau}, \sigma\tau) = ab^{\sigma} a_{\sigma,\tau} u_{\sigma\tau} = ab^{\sigma} u_{\sigma} u_{\tau} = au_{\sigma} bu_{\tau} = h(a,\sigma)h(b,\tau)$. Therefore h is a group homomorphism. Define $t : \bar{G} \to \hat{G}$ as $t(au_{\sigma}) = (a,\sigma)$; [any element of $\bar{G}$ is au for some $a \in A$]. Then clearly toh = Identity and hot = Identity, and so h is an isomorphism. It is easy to verify that the diagram (3) is commutative.

This completes the proof of the proposition. #

Proposition 1.3.4 : The 2-coboundaries correspond to the equivalence class of split extensions.

Proof : Let $1 \to A \to \bar{G} \to G \to 1$ be a split extension. Then $\exists$ a group splitting $G \to \bar{G}$ of $\bar{G} \to G$. Let u_{σ} be the image of σ under this splitting. Then $G \to \bar{G}$ being a homomorphism, $u_{\sigma} u_{\tau} = u_{\sigma\tau}$. Hence the associated cocycle $a_{\sigma,\tau}$ is 1 identically. If now we define $c_{\sigma} = 1$, $\forall\ \sigma \in G$, then $a_{\sigma,\tau} = \frac{c_{\sigma} c_{\tau}^{\sigma}}{c_{\sigma\tau}}$ and hence $a_{\sigma,\tau}$ is a coboundary. Conversely let $a_{\sigma,\tau} = \frac{c_{\sigma} c_{\tau}^{\sigma}}{c_{\sigma\tau}}$ be a 2-coboundary. Let $1 \to A \to \bar{G} \to G \to 1$ be the associated extension. Define $\beta : G \to \bar{G}$ as $\beta(\sigma) = (c_{\sigma}^{-1}, \sigma)$. We have only to show that this is a group homomorphism since it is trivially a splitting. Now $\beta(\sigma)\beta(\tau) = (c_{\sigma}^{-1}, \sigma)(c_{\tau}^{-1}, \tau) = (c_{\sigma}^{-1}(c_{\tau}^{\sigma})^{-1} a_{\sigma,\tau}, \sigma\tau)$. Using (1), one gets $\beta(\sigma)\beta(\tau) = (c_{\sigma\tau}^{-1}, \sigma\tau) = \beta(\sigma\tau)$. Hence the proposition. #

§ 3. Case of a Free Group.

This section deals with an application of the preceding proposition. We show that if G is a free group and if A is any G-module, then $H^2(G,A) = (0)$.

Definition 1.3.1 : We say that a group G is free on a set $S \neq \emptyset$, if (i) S generates G and (ii) if $i: S \to H$ is any map (injection), H being a group, then $\exists$ a unique extension of i to a group homomorphism of $G \to H$. (Notice that G is generated by the image of S under the injection $S \to G$.)

Proposition 1.3.1 : If G is af free group and if A is any G-module, then $H^2(G,A) = (0)$.

Proof : Any element of $H^2(G,A)$ corresponds to a group extension $1 \to A \to \overline{G} \to G \to 1$. Let G be free on a nonempty set S. We choose arbitrary pre-images for elements of S under the mapping $\overline{G} \to G$ to get an injection $S \to \overline{G}$. Since G is free on S, this injection extends to a group homomorphism $G \to \overline{G}$, and clearly this $G \to \overline{G}$ is a splitting of $\overline{G} \to G$ because S generates G. Hence the element we started with in $H^2(G,A)$ is zero.i.e. $H^2(G,A) = (0)$. #

Remark 1.3.1 : We amy note here that as a more general case, if G is a free group and if A is any G-module, then $H^n(G,A) = (0)$ $\forall$ $n \geq 2$, n integer.

Remark 1.3.2. : We end this chapter by proving that if the integers m and n are relatively prime, then any exact sequence of groups $0 \to G \to B \to \pi \to 1$, where $o(G) = m$ and $o(\pi) = n$, splits.

Remark 1.3.3 : To prove this, we require the following result which is proved as Lemma 4.1.3 in Chapter IV : Let π be a finite group of order n and let G be a π-module. Then for any

positive integer i , if $y \in H^i(\pi, G)$, then $ny = 0$.

Remark 1.3.4 : Before going into the proof of the result stated in Remark 1.3.2 , we recall some standard results which we require in the proof : Sylow's first theorem states that if G is a finite group and if ,for a prime p , p^r is the highest power of p which divides $o(G)$, then G has a subgroup of order p^r . Now, if G is a finite group and if H is a subgr-oup of G such that $o(H)$ is the highest power of p which divides $o(G)$, then H is called a p-Sylow subgroup of G . Hence by Sylow's first theorem,every finite group G has a p-Sylow subgroup,for p a prime as above.

In general, a group of order a power of a prime p is called a p-group. A Sylow p-subgroup of a group G is a maximal p-subgroup of G. The second result which we recall here is another theorem of Sylow which states that any two Sylow p-subgroups of a finite group G are conjugate. Finally we recall that if G is a finite p-group , then G has a non-trivial centre.

Proposition 1.3.2 : (Schur-Zassenhaus) : If the integers m and n are relatively prime,then any exact sequence of groups $0 \to G \to B \to \pi \to 1$ where $o(G) = m$ and $o(\pi) = n$, splits.

Proof : Let $0 \to G \xrightarrow{\alpha} B \xrightarrow{\sigma} \pi \to 1$ ---(1) be an exact sequence of groups with $o(G) = m$ and $o(\pi) = n$.

Case 1 : Suppose first that G is abelian. Let $x \in \pi$ be given. Let $\sigma(b) = x$. Consider $f_b : G \to G$ such that $f_b(g) = bgb^{-1}$ for $g \in G$ and $b \in B$ such that $\sigma(b) = x$. Then f_b is an auto-

morphism of G which depends only on x and not on the particular pre-image of x. Now the mapping $\Pi \times G \longrightarrow G$ such that $(x,g) \longmapsto x*g = bgb^{-1}$ where $\sigma(b) = x$, defines a group action of Π on G, and G thus becomes a Π-group. The exact sequence (1) is therefore a group extension and hence corresponds to an element $y \in H^2(\Pi, G)$. Clearly $my = 0$. Again by Remark 1.3.2, $ny = 0$, and since m and n are relatively prime, $y = 0$. The exact sequence (1) therefore corresponds to a 2-coboundary and hence splits by Proposition 1.2.4.

Case 2 : Suppose now that G is not abelian. To show that (1) splits, we are to show that σ has an inverse. It suffices to show that B contains a subgroup L of B such that $o(L) = n$. The proof is by induction on m, the order of G. For $m = 1$, the result is true since in this case $B \cong \Pi$. Assume the result true $\forall\ t < m$ and t relatively prime to n. We shall show the result true for $t = m$. Take a prime p such that p/m. Let P be a maximal p-subgroup of B. Let N = the normaliser of P in $B = \{ b \in B : bPb^{-1} = P \}$. Now the number of conjugates of P in $B = [B:N]$. All these conjugates lie in G, since, for any $x \in B$, $xPx^{-1} \in xGx^{-1}$ since $P < G$; but then $xGx^{-1} = G$ since $G \triangleleft B$. Therefore $xPx^{-1} \in G$. All these are maximal p-subgroups in G and are hence conjugate by a Sylow theorem. Now the normaliser of P in $G = \{x \in G : xPx^{-1} = P\} = G \cap N$ and $[G:G \cap N]$ = the number of conjugates of P in G. Therefore $[G:G \cap N] = [B:N]$.

Now $[B:G\cap N] = [B:G][G:G\cap N]$ and $[B:G\cap N] = [B:N][N:G\cap N]$. Thus $[N:G\cap N] = [B:G] = \frac{o(B)}{o(G)} = o(\pi)$ $= n$. Consider the exact sequence

$0 \to \frac{G\cap N}{P} \to \frac{N}{P} \to \frac{N}{G\cap N} \to 1$ where $o(N/G\cap N) = n$ and $o(G\cap N/P)$ $= t$ where t/m. By the induction hypothesis, $\exists$ $H/P < N/P$ such that $o(H/P) = n$. Let C = Centre P . Then $o(C) \neq 1$. Consider the exact sequence $0 \to P/C \to H/C \to H/P \to 1$ with $o(H/P) = n$ and $o(P/C) < m$ since $o(C) \neq 1$. By the induction hypothesis, $\exists$ a subgroup K/C of H/C such that $o(K/C) = n$. Consider the exact sequence $0 \to C \to K \to K/C \to 1$ where $o(K/C) = n$ and C is abelian. This splits by the abelian case above, so that $\exists$ $L < K$ with $o(L) = n$. This L splits the original exact sequence (1).#

****

CHAPTER II

THEORY OF CENTRAL SIMPLE ALGEBRAS ; THE DEFINITION OF THE BRAUER GROUP OF A FIELD

****

§ 1. Some pre-requisites on Central Simple Algebras .

This section deals with some preliminaries on Central Simple Algebras. The results proved will be used subsequently.

Definition 2.1.1 : Let R be a commutative fing with 1. An R-algebra A is a ring A with the following properties: (i) A is an R-module, (ii) $\forall\ \alpha \in R$ and $\forall\ a,b \in A$, we have $(ab) = a(\alpha b) = (\alpha a)b$.

Remark 2.1.1 : If R = K , a field, then a ring A is a K-algebra of dimension n if (i) A is a vector space of dimension n over K and (ii) $\forall\ \alpha \in K$ and $a,b \in A$, we have $(ab) = a(\alpha b) = (\alpha a)b$.

We may also define an R-algebra in the following way:

Definition 2.1.2 : Let R be a commutative ring with 1 and let A be a ring with 1 . Let $f: R \longrightarrow$ Centre A be a ring homomorphism. If $r \in R$ and $a \in A$, we define a product $r*a = f(r).a$ where . is the multiplication in the ring A. This makes A into an R-module. The ring A together with this R-module structure is called an R-algebra.

Remark 2.1.2 : If K is a field and if R = K and $A \neq 0$ in the above definition, then f is an injection. Thus K can be canonically identified with its image in A

..continued..

under $f : K \to A$. Thus a K-algebra, K being a field, is essentially a ring with centre A containing K.

Remark 2.1.3 : If A and B are R-algebras then $A \otimes_R B$ is in general an R-module. $A \otimes_R B$ becomes a ring under an operation $\phi : (A \otimes_R B) \times (A \otimes_R B) \to A \otimes_R B$ defined as $\phi(a_1 \otimes b_1, a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2$, and $1 \otimes 1$ is the identity of the ring $A \otimes_R B$.

If now $f : R \to A$ and $g : R \to B$ are the corresponding homomorphisms on A and B respectively, then $A \otimes_R B$ is an R-algebra under the ring homomorphism $R \to A \otimes_R B$ such that $x \mapsto f(x) \otimes g(x)$.

Definition 2.1.3 : A ring R with 1 is called simple if it is Artinian and the only two-sided ideals of R are R and (0).

An R-algebra A is called simple if the ring A is simple.

Remark 2.1.4 : We shall denote by $M_n(R)$ the ring of all $n \times n$ matrices with elements in R, R being any ring. We may note here also that $M_n(D)$, for D a division ring, has no proper two-sided ideals.

Remark 2.1.5 : If A and B are finite dimensional K-algebras, for K a field, then $A \otimes_R B$ is a left and right Artinian ring. This is because any descending chain of left or right ideals of $A \otimes_R B$, say $\mathcal{A}_1 \supsetneq \mathcal{A}_2 \supsetneq \cdots \supsetneq \mathcal{A}_n$ is finite since the dimensions of the $\mathcal{A}_i$ as K-subspaces strictly decrease and must therefore terminate.

We now state without proof the following Wedderburn's Theorem, which we shall require subsequently.

Theorem 2.1.1 : Any simple (Artinian) ring is isomorphic to a complete matrix algebra over a division ring.

Definition 2.1.4 : Let K be a field. Let A be a finite dimensional simple K-algebra. If Centre A = K, then A is called a Central Simple K-algebra.

We now prove certain results.

Lemma 2.1.2 : Let K be a field. Let A and B be finite-dimensional associative K-algebras. Let A_1 and B_1 be K-subalgebras of A and B respectively.

Let A_2 = the commutant of A_1 in A

$= \{ x \in A : xa_1 = a_1x \quad \forall \quad a_1 \in A_1 \}$

Let B_2 = the commutant of B_1 in B

$= \{ y \in B : yb_1 = b_1y \quad \forall \quad b_1 \in B_1 \}$

Then $A_2 \otimes_K B_2$ is the commutant of the subalgebra $A_1 \otimes_K B_1$ in A X B .

Proof : Consider any element $a_1 \otimes 1$ of $A_1 \otimes_K 1$. Here $A_1 \otimes 1$ is the image of A_1 under the canonical map $A_1 \to A \otimes_K B$. Let $\{y_i\}_{1 \le i \le n}$ be a K-basis for B. Then any $x \in A \otimes_K B$ has a unique expression $x = \sum_{i=1}^{n} x_i \otimes y_i$, where x_i's $\in A$. If now x commutes with $a_1 \otimes 1$, i.e. if $x(a_1 \otimes 1) = (a_1 \otimes 1)x$ then $\sum_{i=1}^{n} x_i a_1 \otimes y_i = \sum_{i=1}^{n} a_1 x_i \otimes y_i$ so that $x_i a_1 = a_1 x_i \quad \forall \ i \Rightarrow x_i \in A_2 \quad \forall i$.

Now the commutant of $A_1 \otimes_K 1$ in $A \otimes_K B$ is

$\{ x \in A \otimes_K B : x(a_1 \otimes 1) = (a_1 \otimes 1)x \ \forall \ a_1 \in A_1 \}$ =

$\{x \in A \otimes_K B : x = \sum_{i=1}^{n} x_i \otimes y_i$ where $x_i \in A_2$, $y_i \in B\}$ $= A_2 \otimes_K B$. Similarly the commutant of $1 \otimes_K B_1$ in $A \otimes_K B$ is $A \otimes_K B_2$. We now prove that the commutant C of $(A_1 \otimes_K B_1)$ in $A \otimes_K B$ is $(A_2 \otimes_K B) \cap (A \otimes_K B_2)$. One notes that $x \in C \Rightarrow x(a_1 \otimes b_1) = (a_1 \otimes b_1)x$, $\forall\ a_1 \in A_1$ and $b_1 \in B_1 \Rightarrow x(a_1 \otimes 1) = (a_1 \otimes 1)x \Rightarrow x \in A_2 \otimes B$. Similarly $x \in C \Rightarrow x \in A \otimes B_2$ and hence the commutant C is contained in $(A_2 \otimes_K B) \cap (A \otimes_K B_2)$. Conversely let $x \in (A_2 \otimes_K B) \cap (A \otimes_K B_2)$. Then $x(a_1 \otimes b_1) = x(a_1 \otimes 1)(1 \otimes b_1)$ $= (a_1 \otimes 1)x(1 \otimes b_1) = (a_1 \otimes 1)(1 \otimes b_1)x = (a_1 \otimes b_1)x$ $\forall\ a_1 \in A_1$, $\forall\ b_1 \in B_1$. Therefore $x \in C$. Hence $C = (A_2 \otimes_K B) \cap (A \otimes_K B_2)$. Now it is enough to show that $A_2 \otimes_K B_2 = (A_2 \otimes_K B) \cap (A \otimes_K B_2)$. Clearly the L.H.S. $\subset$ R.H.S. . Let $x \in$ the R.H.S. . Let $\{x_i\}_{1 \le i \le r}$ be a K-basis for A_2. We extend this basis to a K-basis of A by introducing $x_{r+1}, x_{r+2}, \ldots, x_n$. Since $x \in A \otimes_K B_2$, $x = \sum_{i=1}^{n} x_i \otimes y_i$ for y_i's $\in B_2$ $\forall$ i. Also $x \in A_2 \otimes_K B$, so $x = \sum_{i=1}^{r} x_i \otimes y_i'$. This shows that $y_i = y_i'$ for $1 \le i \le r$ and $y_{r+1}, y_{r+2}, \ldots, y_n$ are all zero. So $x = \sum_{i=1}^{r} x_i \otimes y_i$, $x_i \in A_2$ and $y_i \in B_2$ $\forall$ i, $1 \le i \le r$. Therefore $x \in A_2 \otimes_K B_2$ so that the R.H.S. $\subset$ L.H.S. Hence the lemma. #

<u>Lemma 2.1.3</u> : Let D and D' be division algebras over K, not necessarily finite dimensional. Let Centre D' = K. Then $D \otimes_K D'$ is a simple K-algebra.

<u>Proof</u> : Let $\mathcal{A}$ be any nonzero two-sided ideal, if any, of $D \otimes_K D'$. Let $\{d_i\}_{i \in I}$ be a K-basis of D. Among all the nonzero elements of $\mathcal{A}$, choose one, say x, of the shortest

expression $x = d_1 \otimes a_1 + d_2 \otimes a_2 + \ldots + d_n \otimes a_n$ where $d_i (1 \leq i \leq n)$ is a part of the basis $\{d_i\}_{i \in I}$ of D and $a_i \in D'$. By considering the element $x(1 \otimes a_1^{-1})$ instead of x, we can assume without loss of generality, that $a_1 = 1$. Let a be any element of D'. Assume $a \neq 0$. Then $(1 \otimes a^{-1})x(1 \otimes a) = d_1 \otimes 1 + d_2 \otimes a^{-1}a_2a + \ldots + d_n \otimes a^{-1}a_na$. Since $\mathcal{A}$ is a two-sided ideal, $y = (1 \otimes a^{-1})x(1 \otimes a) \in \mathcal{A}$. Now $y-x = \sum_{i=2}^{n} d_i \otimes (a^{-1}a_ia - a_i)$ and since $y-x \in \mathcal{A}$ having shorter length than x, we must have $y = x$. i.e. $a_i = a^{-1}a_ia \ \forall\ i,\ 2 \leq i \leq n$. Since this is true for all nonzero $a \in D'$, we conclude that $a_i \in$ Centre $D' = K \ \forall\ i,\ 2 \leq i \leq n$. But then $x = d_1 \otimes 1 + (d_2a_2) \otimes 1 + (d_2a_3) \otimes 1 + \ldots + (d_na_n) \otimes 1 = (d_1 + d_2a_2 + \ldots + d_na_n) \otimes 1 \in D \otimes_K 1$. i.e. x is a nonzero element of the division ring $D \otimes_K 1 \cong D$, and hence is invertible. This implies that $\mathcal{A} = D \otimes_K D'$. Hence $D \otimes_K D'$ is a simple ring and hence a simple K-algebra. #

<u>Lemma 2.1.4</u> : If V and W are f.d. K-spaces, then $(\text{End } V) \otimes_K (\text{End } W) \cong \text{End}(V \otimes_K W)$.

<u>Proof</u> : Let $e_1, e_2, \ldots, e_n$ be a K-basis of V. Define $f_{ij} \in \text{End}_K V$ as $f_{ij}(e_i) = e_j$ and $f_{ij}(e_k) = 0$ if $i \neq k$. The the f_{ij}'s $1 \leq i,j \leq n$, clearly form a K-basis of End V. Suppose the element $\sum_{1 \leq i,j \leq n} f_{ij} \otimes g_{ij}$, where $g_{ij} \in$ End W, is mapped onto zero by the homomorphism θ : $(\text{End } V) \otimes_K (\text{End } W) \to \text{End}(V \otimes_K W)$ given by $(\theta(f \otimes g))(x \otimes y) = f(x) \otimes f(y)$, $\forall\ f \in$ End V, $g \in$ End W, $x \in V$ and $y \in W$. Then if $y \in W$ is arbitrary, we get for a fixed l, $0 = \left(\sum f_{ij} \otimes g_{ij}\right)(e_l \otimes y)$

$= \sum f_{ij}(e_\ell) \otimes g_{ij}(y) = \sum_{1\le j\le n} f_{\ell j}(e_\ell) \otimes g_{\ell j}(y) = \sum_{1\le j\le n} e_j \otimes g_{\ell j}(y)$. Hence $\sum_{1\le j\le n} e_j \otimes g_{\ell j}(y) = 0$. Since $\{e_1, e_2, \ldots, e_n\}$ is a K-basis of V, we must have $g_{\ell j}(y) = 0$, $1\le j\le n$. i.e. $g_{\ell j} = 0$, since y was arbitrary. Since ℓ was also arbitrary, we have $g_{ij} = 0$ $\forall i,j$, $1\le i,j\le n$. This implies that $\sum f_{ij} \otimes g_{ij} = 0$. Therefore the homomorphism θ is one-one. Dimension considerations show that θ is surjective. Hence θ is an isomorphism.#

Lemma 2.1.5 : If R is any K-algebra, then $M_n(K) \otimes_K R \simeq M_n(R)$.

Proof : Consider $f: M_n(K) \otimes_K R \longrightarrow M_n(R)$ given by $f(\sum e_{ij} \otimes r_{ij}) = (r_{ij})$, where $\{e_{ij}\}$ is a canonical basis of $M_n(K)$ and $r_{ij} \in R$. Now f is a homomorphism of rings, for $f((\sum_{i,j} e_{ij} \otimes r_{ij})(\sum_{\ell,k} e_{\ell k} \otimes s_{\ell k})) = f(\sum e_{ij}e_{\ell k} \otimes r_{ij}s_{\ell k}) = f(\sum_{i,j} e_{ij}e_{jk} \otimes r_{ij}s_{jk}) = f(\sum_{i,j} e_{ik} \otimes \sum_j r_{ij}s_{jk}) = (\sum_j r_{ij}s_{jk})(i,k)$

The injectivity and the surjectivity of f is obvious. Therefore f is an isomorphism. #

Proposition 2.1.6 : Let A and B be finite dimensional Central simple K-algebras. Then the K-algebra $A \otimes_K B$ is also Central Simple.

Proof : Since A and B are simple, by Wedderburn's theorem, we can write $A = M_r(D)$ and $B = M_s(D')$ for some integers r and s and division rings D and D'. Now by Proposition 2.1.5, $A = M_r(K) \otimes_K D$ and $B = M_s(K) \otimes_K D'$. So by Lemma 2.1.4, $A \otimes_K B = M_r(K) \otimes_K M_s(K) \otimes_K (D \otimes_K D') = M_{rs}(K) \otimes_K (D \times D') = M_{rs}(K) \otimes_K M_t(D'')$, for some division ring D".

$= M_{rs}(K) \otimes_K M_t(K) \otimes_K D^n = M_{rst}(K) \otimes_K D^n = M_{rst}(D^n)$. Hence $A \otimes B$ is a simple algebra over K. Now Centre $(A \otimes_K B)$ = commutant of $(A \otimes_K B)$ = (Commutant of A in A) $\otimes_K$ (Commutant of B in B) by lemma 2.1.2 = (Centre A) $\otimes_K$ (Centre B) = $K \otimes_K K = K$. Therefore $A \otimes_K B$ is a Central Simple K-algebra .

<u>Corollary 2.1.7</u> : If A is a Central Simple K-algebra and if L is any field extension of K, then $A \otimes_K L$ is Central Simple over L.

<u>Proof</u> : That $A \otimes_K L$ is simple is clear. Also Centre $(A \otimes_K L)$ = Commutant $(A \otimes_K L)$ = (Commutant of A) $\otimes_K$ (Commutant of L) = $K \otimes_K L = L$. #

<u>Proposition 2.1.8</u> : If A is a Central Simple K-algebra, then $A \otimes A^\circ$ is isomorphic to a matrix algebra over K. (Here A° is the opposite algebra of A).

<u>Proof</u> : By Proposition 2.1.6, $A \otimes_K A^\circ$ is a simple K-algebra. We imbed A into $End_K A$ as a vector space, through the left regular representation; i.e. if $a \in A$, we define $L_a \in End_K A$ as $L_a(x) = ax$. The imbedding is $a \longmapsto L_a$. We imbed A° into $End_K A$ through the right regular representation of A; i.e. if $b \in A^\circ$, we define $R_b \in End_K A$ as $R_b(x) = xb$. In this case we are considering the imbedding $b \longmapsto R_b$. Through these ring homomorphisms, A and A° are considered as K-subalgebras of $End_K A$. Notice that $L_a R_b(x) = a(xb)$ and $R_b L_a(x) = (ax)b$. Therefore $L_a R_b = R_b L_a$. We can thus define a nonzero ring homomorphism $f : A \otimes_K A^\circ \longrightarrow End_K A$ as $f(a \otimes b) = L_a R_b$.

The mapping is clearly an abelian group homomorphism. To check that f is a ring homomorphism, we need only to show that $f((a \otimes b)(a' \otimes b')) = f(a \otimes b)f(a' \otimes b')$ $\forall$ $a,a' \in A$ and $\forall$ $b,b' \in A^o$. Now $f((a \otimes b)(a' \otimes b')) = f(aa' \otimes b'b)$ $= L_{aa'}R_{b'b} = L_aL_{a'}R_bR_{b'} = L_aR_bL_{a'}R_{b'} = L_aR_bL_{a'}R_{b'} =$ $f(a \otimes b)f(a' \otimes b')$. Thus f is a ring homomorphism. Consider now the dimensions : $[(A \otimes_K A^o) : K] = [A : K]^2$ and $[\mathrm{End}_K A : K] = [A : K]^2$. Now f is a nonzero homomorphism because the multiplicative identity 1 of $A \otimes_K A^o$ goes the multiplicative identity 1 of $\mathrm{End}_K A$. The kernel f being a two-sided ideal of $A \otimes_K A^o$ is zero, since $A \otimes_K A^o$ is simple. Therefore f is one-one. Since the dimensions agree, f is an isomorphism. #

<u>Proposition 2.1.9</u> : If A is a Central Simple K-algebra, then $[A : K]$ is the square of some integer. (We shall use the abbreviation C.S. for Central Simple).

<u>Proof</u> : We first prove the result for $A = D$, a central divisional algebra over K.

If L is an extension field of K, then $D \otimes_K L$ is a simple algebra over L by lemma 2.1.3 . Take $L = \bar{K}$ (the algebraic closure of K); then $D \otimes_K \bar{K}$ is a matrix ring over a finite dimensional division algebra over $\bar{K}$. Now $D \otimes_K L$ is considered as an L vector-space as follows : if $l \in L$ and $d \otimes a \in D \otimes L$, define $l(d \otimes a) = d \otimes la$. Then $D \otimes_K L$ becomes an L-algebra. Also $[D \otimes_K L : L] = [D : K]$, because, if $x_1, x_2, \ldots, x_n$ is a K-basis of D, then any element of $D \otimes_K L$ has a

unique expression $\sum_{i=1}^{n} x_i \otimes l_i = \sum_{i=1}^{n} l_i(x_i \otimes 1)$. That is, the elements $(x_1 \otimes 1),\ldots,(x_n \otimes 1)$ form an L-basis for $D \otimes_k L$ over L. One notices that $\exists$ no finite dimensional divisional algebra over $\bar{K}$ other than $\bar{K}$ itself : for if D is one such, and if $a \in D$, then $\bar{K}(a)$ is a finite dimensional extension of $\bar{K}$, and hence must be equal to $\bar{K}$, $\bar{K}$ being algebraically closed. Thus $a \in \bar{K}$ showing that $D = \bar{K}$. Hence $D \otimes \bar{K} = M_n(\bar{K})$ and $[D : K] = [D \otimes \bar{K} : \bar{K}] = [M_n(\bar{K}) : \bar{K}] = n^2$. Thus the proposition is true in the case of a division algebra.

If A is arbitrary, we write $A = M_r(K) \otimes D$, where D is a division ring. Then $A \otimes_k \bar{K} = M_r(K) \otimes_k (D \otimes \bar{K}) = M_r(K) \otimes M_n(\bar{K})$, (for some n), $= M_{rn}(\bar{K})$. Therefore $[A : K] = [A \otimes \bar{K} : \bar{K}] = [M_{rn}(\bar{K}) : \bar{K}] = (rn)^2$. Hence the proposition. #

<u>Theorem 2.1.10 (Skolem-Noether)</u> : Suppose A and B are finite dimensional simple algebras over K. Assume that Centre A = K. Then if f and g are two K-algebra monomorphisms of B into A, $\exists$ an invertible element t of A such that $f(x) = t^{-1}g(x)t \quad \forall \; x \in B$.

<u>Proof</u> : Suppose A is a matrix algebra over K. Then f and g give two K-representations of B having the same dimension. By our simple algebra theory, these two representations are equivalent, i.e. $\exists$ an invertible matrix $t \in A = M_n(K)$ such that $f(x) = t^{-1}g(x)t \quad \forall\, x \in B$. Suppose now that A is arbitrary. Then we know that $A \otimes_K A^{\circ} \xrightarrow{\sim} M_n(K)$

for some n. Consider $f \otimes 1_{A^\circ}: B \otimes_K A^\circ \to A \otimes_K A^\circ$ and $g \otimes 1_{A^\circ}: B \otimes_K A^\circ \to A \otimes_K A^\circ$. Now $B \otimes_K A^\circ$ is a simple algebra and by what precedes, we get a $t \in A \otimes A^\circ$ for this case. Considering this for the element $1 \otimes y$, $y \in A^\circ$, we get $1 \otimes y = t^{-1}(1 \otimes y)t$. Therefore $t \in$ Commutant of $1 \otimes_K A^\circ$ in $A \otimes_K A^\circ$. But this commutant = (Commutant of 1 in A) $\otimes_K$ (Commutant of A° in A) = $A \otimes_K K$. Thus $t \in A \otimes_K K$ and hence $t \in A$ since $A \otimes K \cong A$. Applying the result to elements of the type $x \otimes 1$, $x \in B$, we get $f(x) \otimes 1 = t^{-1}(g(x) \otimes 1)t = (t^{-1}g(x)t) \otimes 1$. Therefore $f(x) = t^{-1}g(x)t \ \forall\ x \in B$. #

Corollary 2.1.11 : Any algebra automorphism of a Central Simple K-algebra is an inner automorphism.

Proof : Take A = B and g = identity mapping in the theorem. Then $f(x) = t^{-1}xt$. #

Theorem of the Bi-Commutant 2.1.12 : Let A be a Central Simple K-algebra and let B be a simple subalgebra of A. Let C be the Commutant of B in A. Then the Commutant of C in A is B ; i.e. the bi-commutant (or the Commutant of the Commutant) of B is B itself. Also C is simple and $[A:K] = [B:K][C:K]$.

Proof: Let B be imbedded in $End_K B$, as a K-space through the left regular representation. Then the commutant of the image is isomorphic to B°.

Consider the C.S. K-algebra $End_K B \otimes A$. Now B can be imbedded into this algebra in two ways :

(1) $b \mapsto L_b \otimes 1$, and

(2) $b \mapsto 1 \otimes b$, since B is a subalgebra of A.

Applying the Skolem-Noether's theorem, we conclude that the images are K-isomorphic as algebras through an inner automorphism. Hence their commutants are isomorphic. i.e. $B^\circ \otimes_K A \simeq (\mathrm{End}_K B) \otimes_K C$ since the commutant of 1 is $\mathrm{End}_K B$ and the commutant of b is C. Equating the dimensions, we get $[B^\circ \otimes A : K] = [\mathrm{End}_K B \otimes C : K]$. The L.H.S. $= [A : K][B : K]$ and the R.H.S. $= [\mathrm{End}_K B : K][C : K] = [B : K]^2 [C : K]$. Thus we have $[A : K] = [B : K][C : K]$. Now $B^\circ \otimes A$ is simple so that $\mathrm{End}_K B \otimes_K C$ is simple and therefore C is simple.

Applying what precedes to C in place of B, let C' = commutant of C in A. Then $C' \supset B$ and $[A : K] = [C : K][C' : K]$. But the L.H.S. $= [C : K][B : K]$. Thus $[B : K] = [C' : K]$. Since $C' \supset B$, this implies that $C' = B$. #

<u>Corollary 2.1.13</u> : Let A be a Central Simple K-algebra. Let L be any field extension of K contained in A. Then L is a maximal commutative subring of A $\Leftrightarrow$ L is its own commutant in A $\Leftrightarrow$ $[A : K] = [L : K]^2$.

<u>Proof</u> : Let L be a maximal commutative subring of A. Let L' be the commutant of L in A. If $L' \supsetneq L$, take some $a \in L'$, $a \notin L$. Then $L[a]$ is a commutative subring of A containing L. Hence if L is a maximal commutative subring, we must have $a' \in L$. Contradiction. Therefore $L' = L$. Conversely let $L' = L$. If B is any commutative subring of A containing L, then $B \subset L'$ so that $B = L$. Therefore L is a maximal commutative subring of A.

Assume now that L is a maximal commutative subring. Then $L' = L$ and $[A : K] = [L : K][L' : K] = [L : K]^2$. Conversely if $[A : K] = [L : K]^2$, then $[L : K][L' : K] = [L : K]^2$ so that $[L' : K] = [L : K]$ which together with the fact that $L' \supset L$ implies that $L' = L$. This shows that L is a maximal commutative subring of A. #

Corollary 2.1.14 : If D is a central division algebra over K, then a subfield L is a maximal commutative subfield if and only if $[D : K] = [L : K]^2$. #

====

§2. The Brauer Group of a Field and some related results.

The Brauer Group : Let K be a field and let A and B be Central Simple K-algebras. Then by Wedderburn's Theorem, $A \cong M_n(D)$ for a division ring D and some positive integer n, and $B \cong M_m(D')$ for some division ring D' and positive integer m. Define a relation $\sim$ such that $A \sim B$ if D is K-isomorphic to D' ; (i.e. define A is equivalent to B if D is K-isomorphic to D'). This is clearly an equivalence relation. Let B_K be the set of equivalence classes. We introduce a binary composition on B_K as follows: If A and B are representatives and $\{A\}$ and $\{B\}$ their equivalence classes, we define $\{A\} \times \{B\} = \{A \otimes_K B\}$. This operation is well-defined and makes B_K into a group. Notice first that if $A \sim A_1$ and $B \sim B_1$, then writing $A = M_r(D)$, $A_1 = M_s(D)$,

$B = M_n(D')$, $B_1 = M_m(D')$ we get $A \otimes_k B \simeq M_{rn}(K) \otimes_k (D \otimes_k D')$ and $A_1 \otimes_k B_1 \simeq M_{sm}(K) \otimes_k (D \otimes_k D')$. Since the division rings for $A \otimes_k B$ and $A_1 \otimes_k B_1$ are the same, we conclude that $A \otimes_k B \sim A_1 \otimes_k B_1$. Thus the operation defined above is independent of the representatives chosen.

Associativity : $[\{A\} \times \{B\}] \times \{C\} = \{A \otimes_k B\} \times \{C\} = \{(A \otimes_k B) \otimes_k C\}$ and $\{A\} \times [\{B\} \times \{C\}] = \{A \otimes_k (B \otimes_k C)\}$. Hence the associativity of the operation on B_K follows from the associativity of tensor products.

Identity : The identity element of B_K is $\{K\}$.

Inverse : The inverse of the class $\{A\}$ is the class $\{A^\circ\}$; this follows from the fact that $A \otimes_k A^\circ \simeq$ matrix ring over K. Thus B_K is a group, and is in fact, an abelian group since tensor products commute.

<u>Definition 2.2.1</u> : This group is called the Brauer Group of K.

<u>Proposition 2.2.1</u> : If A is a Central Simple K-algebra of finite K-dimension such that $A \otimes_k L$ is a matrix algebra over L, (here L can be any finite extension of K) then $\exists$ a Central Simple K-algebra of finite dimension, say B, such that $B \sim A$, $B \supset L$ and $[B : K] = [L : K]^2$.

<u>Proof</u> : Notice that since $A \otimes_k L \simeq M_n(L)$, $A^\circ \otimes_k L = (A \otimes_k L)^\circ \simeq (M_n(L))^\circ \simeq M_n(L^\circ) \simeq M_n(L)$ so that $\exists$ a K-vector space say V, of finite L-dimension such that $A^\circ \otimes_k L = \mathrm{End}_L V$. Notice also that $[V : K] < \infty$. Also $\mathrm{End}_L V$ is a subring of $\mathrm{End}_K V$. We compute the commutant of $A^\circ \otimes L$ in $\mathrm{End}_K V$. For this we identify elements of L

with left multiplication on V so that $L \subset \mathrm{End}_K V$ through the imbedding $L \to \mathrm{End}_L V$ given by $l \mapsto f_l$, where $f_l : V \to V$ is such that $f_l(v) = lv$. If $w \in A^\circ \otimes_K L = \mathrm{End}_L V$, then w being an L-linear map of V, for $l \in L$ we have $w.l = l.w$; i.e. upto identification, $w.f_l = f_l.w$ for, $(wf_l)(v) = w(lv) = lw(v) = f_l w(v) = (f_l w)(v)\ \forall\ v \in V$, so that $w.f_l = f_l.w$. Thus L is contained in the commutant of $A^\circ \otimes_K L$. Conversely let w belong to the commutant of $A^\circ \otimes_K L$ so that firstly $w.l = l.w$ for $l \in L$; this shows that w is L-linear, i.e. $w \in \mathrm{End}_L V$. Also w commutes with every element of $A^\circ \otimes_K L$, i.e. of $\mathrm{End}_L V$, so $w \in$ Centre of $\mathrm{End}_L V$, i.e. $w \in L$. Hence we conclude that the Commutant of $A^\circ \otimes_K L$ in $\mathrm{End}_K V$ is L.

Let B be the commutant of A° in $\mathrm{End}_K V$. The Centre of B is nothing but the commutant of B in $\mathrm{End}_K V \cap B$, i.e. $B \cap A^\circ$. Reversing the roles of A° and B, the centre of A° is also $B \cap A^\circ$. This shows that $B \cap A^\circ = K$, so that centre $B = K$. Therefore by Proposition 2.1.6, $A^\circ \otimes_K B$ is a Central Simple K-algebra.

Consider the multiplication map $\theta : A^\circ \otimes_K B \to \mathrm{End}_K V$. Since $A^\circ \otimes_K B$ is simple, kernel $\theta = (0)$ and so θ is injective. Dimension considerations show that θ is surjective, for $[A^\circ \otimes_K B : K] = [A^\circ : K][B:K]$ and $[\mathrm{End}_K V : K] = [V:K]^2$ and these are equal by Theorem 2.1.12.

We now show that the algebra B satisfies the re-

quirements of the Proposition. Since $A^\circ \otimes_k B \xrightarrow{\sim} \mathrm{End}_K V$, B is the inverse class of A°. But A is the inverse class of A°. Therefore B is the same class as A , i.e. $B \sim A$.

Secondly, the commutant of $A^\circ \supset$ the commutant of $A^\circ \otimes_k L = L$. Therefore the commutant of $A^\circ = B \supset L$.

Lastly, $[A^\circ \otimes_k B : K] = [A^\circ : K][B : K] = [V : K]^2$ ---(1). But then $[V : L]^2 = [A^\circ : K]$, since $A^\circ \otimes_k L = \mathrm{End}_L V$, and this implies that $[V : L]^2[L : K]^2 = [A^\circ : K][L : K]^2$, which together with (1) gives that $[A^\circ : K][B : K] = [A^\circ : K][L : K]^2$. Therefore $[B : K] = [L : K]^2$. Hence the Proposition. #

<u>Proposition 2.2.2</u> : Let D be a division ring with centre K such that $[D : K] < \infty$. Then $\exists$ an extension field L of K such that (i) $L \subset D$, (ii) L is separable over K, and (iii) $L \neq K$.

<u>Proof</u> : If characterestic K = 0 , then any extension field of K different from K and contained in D will do.

Let characterestic K = p . It is enough to produce an $x \in D - K$ such that x is separable over K . Suppose no such x exists . Then any $x \in D - K$ is inseparable over K. Thus for $x \in D - K$, $\exists$ an integer $e \geq 1$ and a separable polynomial $f(X) \in K[X]$ such that $f(X^{p^e})$ is the minimum polynomial of x . Now x^{p^e} being a root of the separable polynomial f(X), the extension $K(x^{p^e})$ $(\subset D)$ is separable over K . If degree $f(X) > 1$, then $K(x^{p^e}) \neq K$. Thus $K(x^{p^e})$ satifies the requirements. If degree f(X) = 1 , we assume that $\forall x \in D - K$, $\exists e \geq 1$ such that

$x^{p^e} = a \in K$. Let Ω be a maximal commutative subfield of D, (i.e. Ω is such that $[\Omega : K]^2 = [D : K]$). Then $D \otimes_K \Omega \xrightarrow{\theta} M_n(\Omega)$. Now $\theta(x \otimes 1)^{p^e} = \theta(x^{p^e} \otimes 1) = \theta(a \otimes 1) = \theta[a(1 \otimes 1)] = a\,\theta(1 \otimes 1) = aI_n$, where I_n is the identity $n \times n$ matrix. If $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the eigenvalues of the matrix $\theta(x \otimes 1)$, then the eigenvalues of $\theta(x \otimes 1)^{p^e}$ are $\lambda_1^{p^e}, \lambda_2^{p^e}, \ldots, \lambda_n^{p^e}$. But by what precedes, the eigenvalues of $\theta(x \otimes 1)^{p^e}$ are all equal to a . Hence $\lambda_1^{p^e} = \ldots = \lambda_n^{p^e}$, so that $\lambda_1 = \lambda_2 = \ldots = \lambda_n$. Thus the eigenvalues of $\theta(x \otimes 1)$ are all equal. This is true even if $x \in K$. Hence for $x \in D$, the trace of $\theta(x \otimes 1) = n \times$ the common eigenvalue of $\theta(x \otimes 1)$. Also p/n , for, if e is the least integer such that $x^{p^e} \in K$, then the minimum polynomial of x will be some $x^{p^e} - b$. That is $[K(x) : K]$ is a multiple of p . Also $[K(x) : K] / [D : K]$ and $[D : K] = n^2$. Therefore p / n^2 , and hence p / n .

This shows that the trace $\theta(x \otimes 1) = 0$ if $x \in D$. The elements $\{\theta(x \otimes 1)\}_{x \in D}$ give a system of generators of $M_n(\Omega)$ as an Ω- space . This gives that any element of $M_n(\Omega)$ has trace zero, which is impossible.

This proves that $\exists\ y \in D$, y separable over K and $K(y) \neq K$. Hence the Proposition. #

<u>Proposition 2.2.3</u> : Let D be a division ring with centre K such that $[D : K] < \infty$. Then $\exists$ an extension field L of K having the following properties : (i) $L \subset D$ (ii) $[L : K]^2 = [D : K]$ and (iii) L is separable over K , (i.e. D has

a maximal commutative subfield which is separable over K).

Proof : By the previous Proposition, $\exists$ a field Ω , $\Omega \subset D$ and Ω separable over K, and $\Omega \neq K$. Let D' be the commutant of Ω in D . We notice that D' is a division ring with centre Ω . Now, $[D' : K][\Omega : K] = [D : K]$, and since $[\Omega : K] > 1$, we notice that $[D' : K] < [D : K]$. Again since $[D' : \Omega][\Omega : K] = [D' : K]$ so $[D' : \Omega] < [D : K]$.

By induction we can assume that D' has a subfield L having the following properties : (i) $L \supset \Omega$, L is separable over Ω , and (ii) $[L : \Omega]^2 = [D' : \Omega]$. We now show that L satisfies our requirements. Now, $[L : K]^2 = [L : \Omega]^2 [\Omega : K]^2 = [D' : \Omega][\Omega : K]^2 = [D' : K][\Omega : K] = [D : K]$. Also L is separable over Ω and Ω is separable over K , so that L is separable over K . Hence the Proposition . #

Proposition 2.2.4 : Let A be any Central Simple K-algebra of finite dimension over K . Then there exists a finite Galois Extension Λ of K splitting A , i.e. $\exists$ a finite Galois Extension Λ of K such that $A \otimes \Lambda$ is a matrix algebra over Λ .

Proof : Now $A \cong M_n(D)$ where D is a division ring. By Proposition 2.2.3 , $\exists$ a subfield L of D such that L is separable over K and L is a maximal commutative subfield of D. But then $D \otimes_K L$ must be a matrix ring over L . Let Λ be the least normal extension of K containing L . Then Λ is a finite Galois extension of K . Also since $D \otimes \Lambda \cong (D \otimes_K L) \otimes_L \Lambda$,

$D \otimes_k \Lambda$ is a matrix ring over Λ. Now $A \otimes_k \Lambda = M_n(D) \otimes_k \Lambda = (M_n(K) \otimes_k D) \otimes_k \Lambda = M_n(K) \otimes_k (D \otimes_k \Lambda) = M_n(K) \otimes_k M_m(\Lambda)$, for some m, $= M_{mn}(K \otimes_k \Lambda) = M_{mn}(\Lambda)$. #

****

CHAPTER III

COHOMOLOGICAL INTERPRETATION OF BRAUER GROUPS

***

In this chapter we shall define Galois Cohomology groups, and show that B_K can be interpreted in terms of such Galois Cohomologies.

§ 1. Galois Cohomology :

In this section we define Galois Cohomology in the profinite sense.

Remark 3.1.1 : Let I be a partially ordered set such that given $i,j \in I$, $\exists\ k \in I$, k greater than both i and j with respect to the partial order. This is called being inductively ordered.

Now for each $i \in I$, suppose we are given a group A_i (resp. ring or field). Suppose also for $i \leq j$ there are given homomorphisms $f_{ij} : A_i \longrightarrow A_j$ such that if $i \leq j \leq k$ and f_{ii} = Identity, the situation $A_i \xrightarrow{f_{ij}} A_j \xrightarrow{f_{jk}} A_k$ demands that $f_{jk} \circ f_{ij} = f_{ik}$. We then define the inductive limit, $\varinjlim_{i \in I} A_i$, as follows :-

Consider $\coprod_{i \in I} (A_i \times i)$. We introduce a relation on this as follows : $(x_i,i) \sim (x_j,j)$ if for k both i and j, $f_{ik}(x_i) = f_{jk}(x_j)$. This is an equivalence relation, and under this relation $\sim$ we define $\coprod_{i} (A_i \times i) / \sim \ = \varinjlim_{i \in I} A_i$. We can make $\varinjlim_{i} A_i$ into a group (resp. ring or field) in a natural manner.

We want to see what the composition $\cdot$ is for the 'multiplication' $(x_i,i)\cdot(y_j,j)$. Since $\exists$ $k \geqslant$ both i and j with $f_{ik}(x_i)$, $f_{jk}(y_j)$ both of which belong to A_K, we can talk of $(f_{ik}(x_i)\cdot f_{jk}(y_j), k)$. Define $(x_i,i)\cdot(y_j,j)$ as the equivalence class of $(f_{ik}(x_i)\cdot f_{jk}(y_j), k)$. This makes $\varinjlim_{i \in I} A_i$ into a group.

Remark 3.1.2 : Let L/K be a finite Galois Extension and let $\mathcal{G}_{L/K}$ be its Galois group. Then $\mathcal{G}_{L/K}$ operates on $L^* = L - \{0\}$ and L^* becomes a $\mathcal{G}_{L/K}$-module for, if $\sigma \in \mathcal{G}_{L/K}$, then considering the mapping $\mathcal{G}_{L/K} \times L^* \longrightarrow L^*$ such that $(\sigma,x) \longmapsto \sigma(x) \neq 0$ for $x \in L^*$, we have $\sigma_1\,\sigma_2(x) = \sigma_1(\sigma_2(x))$, $\sigma(x+y) = \sigma(x) + \sigma(y)$ and $\sigma(1) = 1$ $\forall$ $\sigma_1, \sigma_2, \sigma \in \mathcal{G}_{L/K}$. We can therefore talk about $H^2\left(\mathcal{G}_{L/K}, L^*\right)$. Now let M be a finite Galois Extension of K containing L. We notice first that $\mathcal{G}_{L/K} = \mathcal{G}_{M/K} / \mathcal{G}_{M/L}$, so that the mapping $f : \left(\mathcal{G}_{L/K}\right)^2 \longrightarrow L^* \longrightarrow M^*$ induces the mapping $\tilde{f} : \left(\mathcal{G}_{M/K}\right)^2 \longrightarrow M^*$ such that $\tilde{f}(x,y) = f(\bar{x},\bar{y})$ $\forall$ $x,y \in \mathcal{G}_{M/K}$. Consider now a map $\theta : C^2_{\text{hom}}\left(\mathcal{G}_{L/K}, L^*\right) \rightarrow C^2_{\text{hom}}\left(\mathcal{G}_{M/K}, M^*\right)$ such that $\theta(f) = \tilde{f}$. It is easy to verify that θ is a homomorphism and that θ induces a homomorphism $\tilde{\theta} : H^2\left(\mathcal{G}_{L/K}, L^*\right) \rightarrow H^2\left(\mathcal{G}_{M/K}, M^*\right)$. For the latter part, it is enough to show that under θ, cocycles go to cocycles and co-boundaries go to co-boundaries.

Remark 3.1.3 : Let K_S be the separable closure of K in a field algebraic closure of K. (By separable closure we

mean the maximum separable extension or the union of all separable extensions in a fixed algebraic closure of K) . Then the system $\{ H^2(g_{L/K}, L^*) : K \subset L \subset K_S \}$, where L is a finite normal extension of K, is an inductive system. The inducting set is the set of all finite Galois Extensions of K contained in K_S .

<u>Definition 3.1.4</u> : Under the situation of Remark 3.1.3 , we define $H^2_{\text{pro-finite}}(g_{K_S/K}, K_S^*) = \varinjlim H^2(g_{L/K}, L^*)$.

We shall prove later that $B_K \xrightarrow{\sim} H^2_{\text{prof}}(g_{K_S/K}, K_S^*)$, but we first require some results which are given in the next section .

§ 2. <u>Crossed-Product Algebra</u> :

In this section we shall develop the theory of Crossed-Product Algebra with a view to applying it in the proof of $B_K \xrightarrow{\sim} H^2_{\text{prof}}(g_{K_S/K}, K_S^*)$.

Let L/K be a finite Galois Extension. Let $a_{\sigma,\tau}$ be a 2-cocycle of the Galois group $g_{L/K}$ with values in L^* .

Define $A = \sum L u_\sigma$, u_σ being an L-basis. We are defining A as a vector space first. We now define a multiplication as : if $x \in L$ then $u_\sigma x = \sigma(x) u$. For the product of elements of A, we define $\left(\sum x_\sigma u_\sigma\right)\left(\sum y_\sigma u_\sigma\right) = \sum_{\sigma,\tau} (x_\sigma u_\sigma)(y_\tau u_\tau) = \sum x_\sigma \sigma(y_\tau) u_\sigma u_\tau = \sum x_\sigma \sigma(y_\tau) a_{\sigma,\tau} u_{\sigma\tau}$ since $u_\sigma u_\tau = a_{\sigma,\tau} u_{\sigma\tau}$. With this multiplication, A becomes an associative algebra. The associativity follows from the follo-

wing : $\lceil (au_\sigma)(bu_\tau)\rfloor (cu_\rho) = ab^\sigma (u_\sigma u_\tau)cu_\rho = ab^\sigma a_{\sigma,\tau} u_{\sigma\tau}\, cu_\rho$
$= ab^\sigma a_{\sigma,\tau}\, c^{\sigma\tau} a_{\sigma\tau,\rho}\, u_{\sigma\tau\rho}$ ---(1) and $(au_\sigma)\lceil (bu_\tau)(cu_\rho)\rfloor$
$= (au_\sigma)\lceil bc^\tau a_{\tau,\rho}\, u_{\tau\rho}\rfloor = ab^\sigma c^{\sigma\tau} a^\sigma_{\tau,\rho}\, a_{\sigma,\tau\rho}\, u_{\sigma\tau\rho}$ ---(2) .
Comparing (1) and (2), all is accounted for, and the rest is by the cocycle condition. Extending by linearity, A is associative. Also A is an algebra because firstly A is a vector space over K. Secondly, for any $\alpha \in K$, we have
$\alpha\lceil (au_\sigma)(bu_\tau)\rfloor = \alpha\lceil au_\sigma bu_\tau\rfloor = \alpha\lceil ab^\sigma u_\sigma u_\tau\rfloor =$
$\alpha\lceil ab^\sigma a_{\sigma,\tau}\, u_{\sigma\tau}\rfloor = \alpha ab^\sigma a_{\sigma,\tau}\, u_{\sigma\tau}$ ---(3) and
$\lceil \alpha(au_\sigma)\rfloor (bu_\tau) = (\alpha au_\sigma)(bu_\tau) = \alpha au_\sigma bu_\tau = \alpha ab^\sigma u_\sigma u_\tau =$
$\alpha ab^\sigma a_{\sigma,\tau}\, u_{\sigma\tau}$ ---(4) and $(au_\sigma)\lceil \alpha(bu_\tau)\rfloor = (au_\sigma)(\alpha bu_\tau)$
$= au_\sigma \alpha bu_\tau = a\alpha^\sigma u_\sigma bu_\tau = a\alpha^\sigma b^\sigma u_\sigma u_\tau = a\alpha^\sigma b^\sigma a_{\sigma,\tau}\, u_{\sigma\tau} = a\alpha b^\sigma a_{\sigma,\tau} u_{\sigma\tau}$
(since $\alpha \in K$ and σ is a K-automorphism of L) =
$\alpha ab^\sigma a_{\sigma,\tau}\, u_{\sigma\tau}$ ---(5) . Since $\alpha\lceil (au_\sigma)(bu_\tau)\rfloor = \lceil \alpha(au_\sigma)\rfloor (bu_\tau)$
$= (au_\sigma)\lceil \alpha(bu_\tau)\rfloor$, (we may extend this by linearity), A is an algebra over K .

We will show presently that A is a Central Simple split K-algebra with L as its maximal commutative subfield. We however need the following :

<u>Lemma 3.2.1</u> : Let A be a G-group. If $f \in C^2(G,A)$ is a 2-cocycle, then $\exists$ a 2-cocycle g such that (i) f-g is a coboundary, and (ii) $g(1,\sigma) = g(\sigma,1) = 0$.

<u>Proof</u> : Define $h(\sigma) = f(1,\sigma)$. Then h is a 1-cochain. We take $g = f - \partial h$. This g will do, for f and g differ by a coboundary and this gives (i) . We have only to verify (ii) . Now $g(1,\sigma) = f(1,\sigma) - \partial h(1,\sigma) = f(1,\sigma) - \{h(\sigma) - h(\sigma) + h(1)\}$

$= f(1,\sigma) - h(1) = f(1,\sigma) - f(1,1) = 0$ (by the cocycle condition i.e. $a_{1,\sigma} = a_{1,1}$ $\forall\ \sigma$). Also $g(\sigma,1) = f(\sigma,1) - \partial h(\sigma,1)$ $= f(\sigma,1) - \{\sigma h(1) - h(\sigma) + h(\sigma)\}$. Hence $g(\sigma,1) = f(\sigma,1) - \sigma h(1) = f(\sigma,1) - \sigma f(1,1) = 0$ (by the cocycle condition $a_{\sigma,1} = a_{1,1}^{\sigma}$). Hence we get (ii).

Remark 3.2.1 : Let L/K be a finite Galois Extension. let $a_{\sigma,\tau}$ and $b_{\sigma,\tau}$ be equivalent 2-cocycles of $\mathcal{G}_{L/K}$ with values in L*. Then the algebra $A = \sum Lu_{\sigma}$ given by $a_{\sigma,\tau}$ and the algebra $B = \sum Lv_{\sigma}$ given by $b_{\sigma,\tau}$ are K-isomorphic.

Proof : Since $a_{\sigma,\tau}$ is equivalent to $b_{\sigma,\tau}$, $\exists\ c_{\sigma} \in L^*$ such that $a_{\sigma,\tau} = \frac{c_{\sigma} c_{\tau}^{\sigma}}{c_{\sigma\tau}} b_{\sigma,\tau}$ ----(1). Define $f: A \to B$ such that $u_{\sigma} \longmapsto c_{\sigma} v_{\sigma}$, and extend by linearity. Then f is a ring homomorphism. The additivity is clear. For the multiplicativity, $f(u_{\sigma})f(u_{\tau}) = (c_{\sigma} v_{\sigma})(c_{\tau} v_{\tau}) = c_{\sigma} c_{\tau}^{\sigma} b_{\sigma,\tau} v_{\sigma\tau}$ and $f(u_{\sigma} u_{\tau}) = f(a_{\sigma,\tau} u_{\sigma\tau}) = a_{\sigma,\tau} f(u_{\sigma\tau}) = a_{\sigma,\tau} c_{\sigma,\tau} v_{\sigma\tau}$. Using (1), the right hand sides are equal. Also f is a ring isomorphism, and in particular a K-isomorphism.

Let us now first outline what we propose to do :

Remark 3.2.2 : A is already shown to be a K-algebra. We shall first show that A has a multiplicative identity, that A is simple and that Centre A = K. We will then show that the commutant of L in A is L itself, i.e. that L is a maximal commutative subring of A.

Notice that A is a finite dimensional L-vector space and L is a finite dimensional K-vector space, so that A is a finite dimensional K-vector space.

Hence it will thus be

....continued...

shown that A is a finite dimensional Central Simple K-algebra with L as its maximal commutative subfing.

In particular, if L is a maximal commutative subring of A we will have $[A:K] = [L:K]^2$ ---(1), by Corollary 2.2.13. But then $[A:K] = [A:L][L:K]$ and so (1) will imply that $[A:L][L:K] = [L:K]^2$ which will give $[A:L] = [L:K]$. Further, $o(\mathcal{G}_{L/K}) = [L:K] = [A:L]$.

Remark 3.2.3 : Thereafter we will show that A is a split K-algebra, (i.e. $A \cong$ a matrix ring over K), if and only if the two cocycle $a_{\sigma,\tau}$ is equivalent to the trivial 2-cocycle $b_{\sigma,\tau} = 1 \ \forall \sigma, \tau$. To do this we employ the following procedure : Let $A_{a_{\sigma,\tau}}$ (notation) denote " A with the cocycle $a_{\sigma,\tau}$," and let $A_{trivial}$ denote " A with the trivial 2-cocycle $b_{\sigma,\tau} = 1 \ \forall \sigma, \tau$." We will first show that $A_{trivial} \cong M_n(K)$ --(2) where $n = [L:K]$. Then for the first part of the proof, we assume that $a_{\sigma,\tau} \sim b_{\sigma,\tau}$ and prove that $A_{trivial} \cong A_{a_{\sigma,\tau}}$---(3). Thus the one way implication will be proved, because (2) and (3) together imply that $A_{a_{\sigma,\tau}} \cong M_n(K)$ if $a_{\sigma,\tau} \sim b_{\sigma,\tau}$. For the converse we assume that $A_{a_{\sigma,\tau}} \cong M_n(K)$---(4). But then (2) and (4) give that $A_{trivial} \cong A_{a_{\sigma,\tau}}$. The proof then that $a_{\sigma,\tau}$ is now equivalent to $b_{\sigma,\tau}$ will follow from a Proposition below, i.e. Proposition 3.2.2.

We now proceed to prove these results :

Claim I : A has a multiplicative identity.

Suppose $A = \sum Lu_\sigma$ corresponding to the cocycle $a_{\sigma,\tau}$ with the property that $a_{\sigma,1} = a_{1,\sigma} = \text{Identity } \forall\sigma$. Now u_1 is the multiplicative identity for A for, if $x \in L$, then $u_1 x = x = x u_1$ (after identification of L with Lu_1 through the isomorphism $l \mapsto l u_1$.) Also $u_1 u_\sigma = a_{1,\sigma} u_\sigma = u_\sigma$ since $a_{1,\sigma} = 1$ and $u_\sigma u_1 = a_{\sigma,1} u_\sigma = u_\sigma \ \forall\sigma$. Thus u_1 is the multiplicative identity for A .

To prove this for A with any 2-cocycle $a_{\sigma,\tau}$, we find an equivalent cocycle $b_{\sigma,\tau}$ and the property that $b_{\sigma,1} = b_{1,\sigma}$ = Identity $\forall\sigma$. Then by Remark 3.2.1, the algebra $A = \sum Lu_\sigma$ given by $a_{\sigma,\tau}$ and the algebra $B = \sum Lv_\sigma$ given by $b_{\sigma,\tau}$ are ring isomorphic. But by the above, B has a multiplicative identity. Therefore A has a multiplicative identity.

<u>Claim II</u> : Centre A = K.

Assume that u_1 is the identity for A . Let $x \in A$ such that $x \in$ Centre A . We write $x = \sum x_\sigma u_\sigma$, $x_\sigma \in L$. Then $\forall\, l \in L$, $lx = xl$. Now $lx = \sum l x_\sigma u_\sigma$ and $xl = \sum x_\sigma u_\sigma l = \sum x_\sigma \sigma(l) u_\sigma$. Since u_σ is a basis for the algebra, comparing coefficients, $l x_\sigma = x_\sigma \sigma(l)$. If $x_\sigma \neq 0$ then $\sigma(l) = l \ \forall\sigma \Rightarrow \sigma = $ Identity; i.e. $x_\sigma = 0$ if $\sigma \neq$ Identity. Hence $x = x_1 u_1$. Also $u_\sigma x = x u_\sigma$, but then $u_\sigma x = \sigma(x) u_\sigma = x u_\sigma \Rightarrow \sigma(x) = x \ \forall\sigma \Rightarrow x \in K$. Therefore Centre $A \subset K$, and hence Centre $A = K$. This proves our Claim II.

<u>Claim III</u> : The commutant of L in A is L itself .

Let $x \in$ the commutant of L. Write $x = \sum l_\sigma u_\sigma$. Take any $l \in L$. Then $lx = xl$ since $x \in$ the commutant of L. Now $xl = \sum l_\sigma u_\sigma l = \sum l_\sigma \sigma(l) u_\sigma$ and $lx = \sum l l_\sigma u_\sigma$. Since u_σ is a basis, comparing coefficients, $l_\sigma \sigma(l) = l l_\sigma$. Therefore $\sigma(l) = l$ if $l_\sigma \neq 0$, $\forall\, l \in L$ and so $\sigma =$ Identity if $l_\sigma \neq 0$; i.e. $l_\sigma = 0$ if $\sigma \neq$ Identity. Hence $x = l_1 u_1 \in L u_1$ (we can take $u_1 =$ Identity element). Therefore the commutant of L in $A \subseteq L$. Conversely $L \subseteq$ Commutant of L trivially, and so Commutant of L in A is L.

Claim IV : A is simple.

Let $\mathcal{A}$ be a nonzero two-sided ideal of A. We will show that $\mathcal{A} = A$. Choose any $a \in A$ with $a \neq 0$. Write $a = l_1 u_{\sigma_1} + l_2 u_{\sigma_2} + \ldots + l_r u_{\sigma_r}$, $(l_1 \neq 0)$ where a is such that r is least. Suppose $r > 1$. Let $l \in L$ such that $\sigma_1(l) \neq \sigma_2(l)$, (since σ_1 and σ_2 are distinct). Now $al = l_1 u_{\sigma_1} + \ldots + \ldots = l_1 \sigma_1(l) u_{\sigma_1} + \ldots + \ldots$, and $al \in \mathcal{A}$ since $\mathcal{A}$ is a two-sided ideal. This implies that $(\sigma_1(t))^{-1} al \in \mathcal{A}$. But $\sigma_1(l)^{-1} al = l_1 u_{\sigma_1} + \ldots + \ldots$, so that $a - \sigma_1(l)^{-1} al =$ something which has at most $r-1$ summands, and this element lies in $\mathcal{A}$, contradicting the minimality of r. Hence $r = 1$; i.e. $a = l_1 u_{\sigma_1}$. We show that the u_{σ_i}'s are units in A. Now $u_\sigma u_{\bar{\sigma}^{-1}} = a_{\sigma, \bar{\sigma}^{-1}} u_1$. But u_1 is identity and $a_{\sigma, \bar{\sigma}^{-1}} \in L^*$. So u_σ is a unit in A. This implies that a is a unit of A, since $a = l_1 u_{\sigma_1}$. Therefore $\mathcal{A} = A$. Thus A is simple.

Claim V : A is a split K-algebra $\Leftrightarrow$ the 2-cocycle $a_{\sigma,\tau}$

is equivalent to the trivial 2-cocycle $b_{\sigma,\tau} = 1 \ \forall \ \sigma, \tau$.

Firstly to show that $A_{trivial} \simeq M_n(K)$, where $n = [L : K]$, we set up a map $f : A \longrightarrow Hom_K(L,L)$ as $f(au_\sigma) = \lambda_a \cdot \sigma$, where λ_a is homothecy by a. (Elements of A are linear combinations of au_σ's). Now f is a ring homomorphism. The additivity is clear. Also $f((au_\sigma)(bu_\tau)) = f(ab^\sigma u_{\sigma\tau}) = \lambda_a \lambda_{b^\sigma} \circ \sigma\tau$ (using $b_{\sigma,\tau} = 1$). But $(\lambda_a \circ \sigma)(\lambda_b \circ \tau) = \lambda_a \circ \lambda_{b^\sigma} \circ \sigma\tau$. Therefore f is a ring homomorphism. Here f is not the zero map because the identity of A goes to the identity of $Hom_K(L,L)$. Also, kernel f being a two-sided ideal, must be (0). Therefore f is 1-1. Dimension considerations show that f is bijective ; (both have K-dimension $[L : K]^2$). Therefore f is an isomorphism and so $A_{trivial} \simeq M_n(K)$.

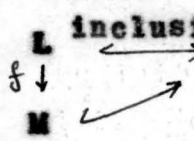
Assuming that $a_{\sigma,\tau}$ is equivalent to $b_{\sigma,\tau}$, by Remark 3.2.1 , we know that $A_{trivial} \simeq A_{a_{\sigma,\tau}}$. These together imply that $A_{a_{\sigma,\tau}} \simeq M_n(K)$ if $a_{\sigma,\tau} \sim b_{\sigma,\tau}$. Thus the one way implication of Claim V (i.e. Remark 3.2.3) is proved.

For the converse, we know that $A_{trivial} \simeq M_n(K)$, $n = [L : K]$. If we assume now that $A_{a_{\sigma,\tau}} \simeq M_n(K)$, then $A_{a_{\sigma,\tau}} \simeq A_{trivial}$. The fact that $a_{\sigma,\tau}$ is equivalent to the trivial 2-cocycle follows from the following

<u>Proposition 3.2.2</u> : Let $A = \sum Lu_\sigma$ with the cocycle $a_{\sigma,\tau}$ and let $B = \sum Lv_\sigma$ with the cocycle $b_{\sigma,\tau}$. Then $A \simeq B$ as K-algebras $\Leftrightarrow$ $a_{\sigma,\tau} \sim b_{\sigma,\tau}$.

<u>Proof</u> : By Remark 3.2.1 , the $\Leftarrow$ implication has already

been proved. For the converse, let $f: A \to B$ be the given K-isomorphism. Let $f(L) = M$. Now M is a subfield of B. Also since $f(A) = B$ so $B = \sum_{\sigma \in g_{L/K}} Mf(u_\sigma)$. We have



Using the Skolem-Noether theorem, $\exists$ an inner automorphism say p of B such that pof = Identity on L. Let $w_\sigma = (pof)(u_\sigma)$. Applying p to B, we get $B = \sum Lw_\sigma$, using the fact that $B = \sum_{\sigma \in g_{L/K}} Mf(u_\sigma)$. We now want to see the multiplication in terms of the new basis w_σ of B. For $x \in L$, we have $u_\sigma x = \sigma(x)u_\sigma$. Applying f to each side, the L.H.S. $= f(u_\sigma x) = f(u_\sigma)f(x)$, since f is a homomorphism, and the R.H.S. $= f(\sigma(x))f(u_\sigma)$. Applying p to each, $pof(u_\sigma x) = (pof(u_\sigma))((pof)(x)) = w_\sigma x$ and $po[f(\sigma(x))f(u_\sigma)] = (pof)(\sigma(x))((pof)(u_\sigma)) = \sigma(x)w_\sigma$. Thus $w_\sigma x = \sigma(x)w_\sigma$. Next, starting with $u_\sigma u_\tau = a_{\sigma,\tau} u_{\sigma\tau}$, we get $f(u_\sigma u_\tau) = f(a_{\sigma,\tau} u_{\sigma\tau}) \Rightarrow f(u_\sigma)f(u_\tau) = f(a_{\sigma,\tau})f(u_{\sigma\tau})$. Applying p to each side $w_\sigma w_\tau = a_{\sigma,\tau} w_{\sigma\tau}$. We want to show that the element $w_\sigma o\, v_\sigma^{-1}$, which belongs to B since v_σ is a unit, commutes with all elements of L. This will show that $w_\sigma o\, v_\sigma^{-1} \in L$. We have, $w_\sigma x = \sigma(x)w_\sigma$ for $x \in L$; also $v_\sigma x = \sigma(x)v_\sigma$. We want to show that $w_\sigma o\, v_\sigma^{-1} x = x w_\sigma o\, v_\sigma^{-1}$ $\forall$ $x \in L$; i.e. to show that $w_\sigma o\, v_\sigma^{-1} x v_\sigma = x w_\sigma$ $\forall$ $x \in L$. Writing $x = \sigma(y)$, the L.H.S. $= w_\sigma o\, v_\sigma^{-1}\sigma(y)v_\sigma = w_\sigma o v_\sigma^{-1} v_\sigma(y)$ $= w_\sigma y$, and the R.H.S. $= \sigma(y)w_\sigma = w_\sigma y$. Therefore $w_\sigma o\, v_\sigma^{-1} x = x w_\sigma o\, v_\sigma^{-1}$ $\forall$ $x \in L$, so that $w_\sigma o\, v_\sigma^{-1} \in L$; i.e. we can write $w_\sigma o\, v_\sigma^{-1} = c_\sigma \in L^*$, for some element c_σ in L^* since v_σ and

w_σ are units, so that $w_\sigma = c_\sigma v_\sigma$. Now, the cocycle with the basis $c_\sigma v_\sigma = w_\sigma$ will be $\frac{c_\tau c_\tau^\sigma}{c_{\sigma\tau}} \times$(the cocycle for the basis v_σ), i.e. $\frac{c_\tau c_\tau^\sigma}{c_{\sigma\tau}} \times (b_{\sigma,\tau})$. But with the basis w_σ, the cocycle for B is $a_{\sigma,\tau}$. Therefore the cocycle $a_{\sigma,\tau} = \frac{c_\sigma c_\tau^\sigma}{c_{\sigma\tau}} \times b_{\sigma,\tau}$. Thus $a_{\sigma,\tau}$ is equivalent to $b_{\sigma,\tau}$. Hence the proposition. #

Our object now is to prove the following main theorem of this section :

<u>Theorem 3.2.3</u> : Let L/K be a finite Galois Extension. Let $A = \sum Lu_\sigma$ corresponding to the 2-cocycle $a_{\sigma,\tau}$, and let $B = \sum Lv_\sigma$ corresponding to the 2-cocycle $b_{\sigma,\tau}$. Then $A \otimes_K B$ is equivalent to the algebra determined by the cocycle $a_{\sigma,\tau} . b_{\sigma,\tau}$. (in the sense of Brauer Equivalence).

The proof of the Theorem requires the following

<u>Lemma 3.2.4</u> : Let A be a finite dimensional simple K-algebra. Let e be an idempotent in A , $e \neq 0$. Then eAe is a simple K-algebra equivalent to A .

<u>Proof of the Lemma</u> : Since A is simple, by Wedderburn's theorem, $A = M_n(D)$ for some division ring D; i.e. $A = End_D V$, where V is a right D-vector space. Since $e \in A$, e can be considered as a D-endomorphism of V . Also A operates on V on the ~~right~~ left such that if $w \in A$ and $d \in D$, $v \in V$, then $w(vd) = w(v)d$ ---(1). Here eV and $(1 - e)V$ are D-subspaces of V because of (1),for, if $x \in eV$ then $x = ev$ for some $v \in V$. So $xd = e(v)d = e(vd) \in eV$. Therefore eV is a D-subspace of V . Similarly $(1-e)V$ is a D-subspace of V and we can also

SHOW show that $V = eV \oplus (1-e)V$.

Choose now a D-basis $x_1, x_2, \ldots, x_r$ of eV and a D-basis $y_1, y_2, \ldots, y_s$ of $(1-e)V$. Then $x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_s$ is a D-basis of V. We compute the matrix of e with respect to this D-basis of V. Now $ex_i = e(ev_i)$ where $x_i = ev_i$ for $v_i \in V$ since $x_i \in eV$. Therefore $ex_i = e(ev_i) = e^2 v_i = ev_i = x_i \ \forall\, i$, $1 \leq i \leq r$. Also $ey_j = e((1-e)w_j)$, where $y_j = (1-e)w_j$ for $w_j \in V$. Therefore $ey_j = (e-e^2)w_j = 0$. So the matrix of e is diagonal $(\overbrace{1,1,1,\ldots,1}^{r \text{ times}}, \overbrace{0,0,0,\ldots,0}^{s \text{ times}})$. Using block multiplication of matrices, $eM_n(D) =$

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} P & Q \\ R & S \end{pmatrix}\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} P & 0 \\ R & 0 \end{pmatrix} = \begin{pmatrix} P & 0 \\ 0 & 0 \end{pmatrix}$$

So $eM_n(D)e$ = set of matrices of the type $\begin{pmatrix} P & 0 \\ 0 & 0 \end{pmatrix}$ where P is an $r \times r$ matrix over D. Thus $eM_n(D)e$ is isomorphic to $M_r(D)$. Now $A \sim D$ by definition, and also $M_r(D) \sim D$. But then $M_r(D) \xrightarrow{\sim} eAe$. Hence $eAe \sim A$. Hence the Lemma.#

<u>Proof of Theorem 3.2.3</u> :

We note that $A \otimes_K B$ is a central simple K-algebra. Also $L \otimes_K L$ is a commutative subring of $A \otimes_K B$. We will find an idempotent $e \in L \otimes_K L$, $e \neq 0$, such that $e(A \otimes_K B)e$ is equivalent to the algebra $\sum Lw_\sigma$ corresponding to the 2-cocycle $a_{\sigma,\tau} \cdot b_{\sigma,\tau}$. By lemma 3.2.4, we will have $A \otimes_K B \sim e(A \otimes_K B)e$. Hence the above statement will imply that $A \otimes_K B \sim \sum Lw_\sigma$ corresponding to the 2-cocycle $a_{\sigma\tau} \cdot b_{\sigma\tau}$,

...continued...

and we will be through.

Now L being a separable extension of K, $\exists$ some $t \in L$ such that $L=K(t)$. Let $F(x)$ be the minimal polynomial of t over K. Let $[L:K] = n$ so that degree $F = n$.

Define $e = \frac{\prod_{\sigma\neq 1}[(t \otimes 1) - (1 \otimes \sigma t)]}{\prod_{\sigma\neq 1}(t - \sigma t) \otimes 1}$. Clearly $\prod_{\sigma\neq 1}(t \otimes 1 - 1 \otimes \sigma t) \in L \otimes_K L$. Also since L/K is separable and t generates L/K so $\sigma t \neq t \ \forall \sigma \neq 1$, so that $\prod_{\sigma\neq 1}(t-\sigma t) \neq 0$. Hence $\prod_{\sigma\neq 1}(t-\sigma t) \otimes 1$ is a nonzero element of $L \otimes 1 \cong L$, and is hence invertible. Therefore $e \in L \otimes_K L$. We will show that e is an idempotent ($e \neq 0$).

Consider $(t \otimes 1 - 1 \otimes t)e = \frac{\prod_{\tau}(t \otimes 1 - 1 \otimes \tau t)}{\prod_{\tau\neq 1}(t - \tau t) \otimes 1}$.

The numerator $= t^n \otimes 1 - t^{n-1} \otimes f_1 + t^{n-2} \otimes f_2 - \ldots\ldots$, where $f_1, f_2, \ldots$ are elementary symmetric functions of τt, $\tau \in \mathcal{G}_{L/K}$. Now $f_1, f_2, f_3, \ldots$ being elementary symmetric fubctions in τt, we get $f_1, f_2, \ldots$ belong to K. So for each i, $t^{n-i} \otimes f_i = t^{n-i} f_i \otimes 1$, so that $t^n \otimes 1 - t^{n-1} \otimes f_1 + t^{n-2} \otimes f_2 \ldots\ldots$ $= (t^n - f_1 t^{n-1} + f_2 t^{n-2} - \ldots.) \otimes 1 = 0$, since t satisfies the polynomial $F(x) = \prod_{\tau\in\mathcal{G}_{L/K}}(x - \tau t)$, the roots of F(x) being all the τt, $\tau \in \mathcal{G}_{L/K}$. Therefore the numerator is zero, i.e. $(t \otimes 1 - 1 \otimes t)e = 0$ so that $(t \otimes 1)e = (1 \otimes t)e$. Also any $y \in L$ is of the form $\sum_{i=0}^{n-1} a_i t^i$, for $a_i \in K$. Hence $(y \otimes 1)e = [(\sum a_i t^i) \otimes 1]e = \sum(a_i t^i \otimes 1)e = \sum a_i(t^i \otimes 1)e = \sum a_i(t \otimes 1)^i e = \sum a_i(1 \otimes t)^i e = \sum a_i(1 \otimes t^i)e = \sum(1 \otimes a_i t^i)e = (1 \otimes \sum a_i t^i)e = (1 \otimes y)e$.

Thus $(y \otimes 1)e = (1 \otimes y)e$, for $y \in L$. Again $e^2 = \frac{[\prod_{\sigma\neq 1}(t \otimes 1 - 1 \otimes \sigma t)]e}{\prod_{\sigma\neq 1}(t - \sigma t) \otimes 1}$

$= \dfrac{\prod (t \otimes 1 - \sigma t \otimes 1)e}{\prod (t - \sigma t) \otimes 1} = \dfrac{\prod_{\sigma \neq 1} \{(t - \sigma t) \otimes 1\} e}{\prod_{\sigma \neq 1} (t - \sigma t) \otimes 1} = e$. Therefore e is an idempotent. To show that $e \neq 0$, we see that the numerator of the expression for e is $t^{n-1} \otimes 1 - t^{n-2} \otimes g_1 + t^{n-3} \otimes g_2 - \ldots\ldots$, where $g_1, g_2, \ldots$ are certain elements of L. This is nonzero since $1, t, t^2, \ldots, t^{n-1}$ is a K-basis of L.

Consider now $e(A \otimes_k B)e$. Now $A \otimes_k B = (\sum Lu_\sigma) \otimes_k (\sum Lv_\sigma)$ $= \sum (L \otimes_k L)(u_\sigma \otimes v_\tau)$, σ and τ running independently over $\mathcal{G}_{L/K}$ in this summation. Thus $e(A \otimes_k B)e = \sum e(L \otimes L)(u_\sigma \otimes v_\tau)e$ $= \sum [e(L \otimes 1)e][e(1 \otimes L)e][e(u_\sigma \otimes v_\tau)e]$. Notice that $e(L \otimes 1)e = e(1 \otimes L)e$ by what was proved earlier. Also $e(L \otimes 1)e$ is K-isomorphic to L, the isomorphism being $l \mapsto e(l \otimes 1)e$. Hence $e(A \otimes B) = \sum L' w_\sigma$ where $L' = e(L \otimes 1)e$ and $w_\sigma = e(u_\sigma \otimes v_\tau)e$. We will now compute the 2-cocycle with respect to w_σ, using the fact that $u_\sigma y = \sigma(y) u_\sigma$ and $v_\tau(z) = \tau(z) v_\tau$ for $y \in A$, $z \in B$ ---(1).

Claim : $e(u_\sigma \otimes v_\tau)e = 0$ if $\sigma \neq \tau$

$=$ either of $e(u_\sigma \otimes v_\sigma)$ or $(u_\sigma \otimes v_\sigma)e$ if $\sigma = \tau$.

Now $e(u_\sigma \otimes v_\tau) = \dfrac{\prod_{\rho \neq 1} (t \otimes 1 - 1 \otimes \rho t)}{\prod_{\rho \neq 1} (t - \rho t) \otimes 1} (u_\sigma \otimes v_\tau)$ ---(2).

This is the sum of elements of the form $\dfrac{x \otimes y}{a \otimes 1} u_\sigma \otimes v_\tau$ which is equal to $(xa^{-1} \otimes y)(u_\sigma \otimes v_\tau) = x a^{-1} u_\sigma \otimes y v_\tau =$ $u_\sigma \sigma^{-1}(xa^{-1}) \otimes v_\tau \tau^{-1}(y)$ [we use (1)], $= u_\sigma \sigma^{-1}(x) \sigma^{-1}(a^{-1}) \otimes v_\tau \tau^{-1}(y) = \dfrac{u_\sigma \sigma^{-1}(x) \otimes v_\tau \tau^{-1}(y)}{\sigma^{-1}(a) \otimes 1} = \dfrac{(u_\sigma \otimes v_\tau)(\sigma^{-1}(x) \otimes \tau^{-1}(y)}{\sigma^{-1}(a) \otimes 1}$.

Thus the R.H.S. of (2) $= (u_\sigma \otimes v_\tau) \dfrac{\prod_{\rho \neq 1} (\sigma^{-1}t \otimes 1 - 1 \otimes \tau^{-1}\rho\, t)}{\prod_{\rho \neq 1} (\sigma^{-1}t - \sigma^{-1}\rho\, t) \otimes 1}$.

Suppose now $\sigma \neq \tau$. Then taking $\rho = \tau\sigma^{-1}$, we have $\rho \neq$ Identity and $\sigma^{-1}t - \tau^{-1}\rho\, t = \sigma^{-1}t - \tau^{-1}\tau\,\sigma^{-1}t = \sigma^{-1}t - \sigma^{-1}t = 0$. Hence in this case $e(u_\sigma \otimes v_\tau)e = 0$. Let $\sigma = \tau$. Then $e(u_\sigma \otimes v_\tau)e = (u_\sigma \otimes v_\sigma)e$. Similarly we can prove that $e(u_\sigma \otimes v_\tau)e = e(u_\sigma \otimes v_\sigma)$. Hence $e(A \otimes_k B)e = \sum L'w_\sigma$ where $w_\sigma = e(u_\sigma \otimes v_\sigma)e$. Now let $e(l \otimes 1)e \in L' = e(L \otimes 1)e$. Then $w_\sigma [e(l \otimes 1)e] = (u_\sigma \otimes v_\sigma)(e(l \otimes 1)e) = e(u_\sigma \otimes v_\sigma)(l \otimes 1)e$, (by switching e) , $= e(u_\sigma l \otimes v_\sigma)e = e(\sigma(l)u_\sigma \otimes v_\sigma)e = e(\sigma(l) \otimes 1)(u_\sigma \otimes v_\sigma)e = [e(\sigma(l) \otimes 1)e][e(u_\sigma \otimes v_\sigma)e] = e(\sigma(l) \otimes 1)w_\sigma$. Also $w_\sigma w_\tau = e(u_\sigma \otimes v_\sigma)e^2(u_\tau \otimes v_\tau)e = e(u_\sigma u_\tau \otimes v_\sigma v_\tau)e = e(a_{\sigma,\tau}u_{\sigma\tau} \otimes b_{\sigma,\tau}v_{\sigma,\tau})e = e[(a_{\sigma,\tau} \otimes b_{\sigma,\tau})(u_{\sigma\tau} \otimes v_{\sigma\tau})]e = e[(a_{\sigma,\tau} \otimes b_{\sigma,\tau})e(u_{\sigma\tau} \otimes v_{\sigma\tau})]e = e(a_{\sigma,\tau} \otimes b_{\sigma,\tau})ew_{\sigma\tau} = [e(a_{\sigma,\tau}\, b_{\sigma,\tau} \otimes 1)e]w_{\sigma\tau}$. Hence the cocycle for the basis w_σ will be $e(a_{\sigma,\tau}\, b_{\sigma,\tau} \otimes 1)e$, (i.e. the coefficient of $w_{\sigma\tau}$) . This can be identified with the element $a_{\sigma,\tau}b_{\sigma,\tau}$ of L under the canonical isomorphism $L' \longrightarrow L$ such that $e(l \otimes 1)e \longmapsto l$.

Hence the cocycle for the algebra $\sum L'w_\sigma$ is $a_{\sigma,\tau}b_{\sigma,\tau}$ i.e. the cocycle for the algebra $e(A \otimes_k B)e$ is $a_{\sigma,\tau}b_{\sigma,\tau}$.

Hence the proof. #

---

§ 3.

In this section we will prove that

$$B_K \simeq H^2_{prof}\left(\mathcal{G}_{K_S/K}, K_S^*\right) \quad .$$

Remark 3.3.1 : Before we go into this proof, we first recall the following two results which have been proved in § 2 :

(a) Let L/K be a finite Galois Extension. Let $a_{\sigma,\tau}$ be a 2-cocycle of the Galois group $\mathcal{G}_{L/K}$ with values in L^*. Then defining $A = \sum_{\sigma \in \mathcal{G}_{L/K}} Lu_\sigma$ as we did in the previous section, we have shown that A is a finite dimensional Central Simple K-algebra with L as its maximal commutative subring.

(b) We have also shown that if L/K is a finite Galois Extension, and if $A = \sum Lu_\sigma$ corresponding to the 2-cocycle $a_{\sigma,\tau}$ and $B = \sum Lv_\sigma$ corresponding to the 2-cocycle $b_{\sigma,\tau}$, then $A \otimes_K B$ is equivalent to the algebra $\sum Lw_\sigma$ corresponding to the cocycle $a_{\sigma,\tau} \cdot b_{\sigma,\tau}$.

Remark 3.3.2 : We notice also that if K is a field and L any extension of K, then $\exists$ a natural homomorphism $B_K \to B_L$ as follows :

If A is a finite dimensional Central Simple K-algebra, then $A \otimes_K L$ is a finite dimensional Central Simple L-algebra. Hence $\{A\} \longmapsto \{A \otimes_K L\}$ gives a map $B_K \to B_L$.

Also since $(A \otimes_K B) \otimes_K L \simeq (A \otimes_K L) \otimes_L (B \otimes_K L)$, the above map is a group homomorphism. We will denote by $B_{L/K}$, the kernel of the homomorphism $B_K \to B_L$.

Remark 3.3.3 : From Proposition 2.2.4 , we have seen that if A is a Central Simple K-algebra of finite dimension, then $\exists$ a finite Galois Extension Λ of K such that $A \otimes_K \Lambda$ is a matrix algebra over Λ .

This implies that A belongs to the kernel of $B_K \to B_\Lambda$, i.e. $A \in B_{\Lambda/K}$, so that $B_K \subset \bigcup B_{L/K}$, the union running over all finite Galois Extension L over K. But then $\bigcup B_{L/K} \subset B_K$, and thus $B_K = \bigcup B_{L/K}$.

Proposition 3.3.1 : If L is a finite Galois Extension of K, then $\exists$ a natural isomorphism $H^2\left(\mathcal{G}_{L/K}, L^*\right) \longrightarrow B_{L/K}$.

Proof : Consider the map $\theta : H^2\left(\mathcal{G}_{L/K}, L^*\right) \longrightarrow B_{L/K}$ such that $a_{\sigma,\tau} \longmapsto A = \sum L u_\sigma$.

Now under θ , $a_{\sigma,\tau} \longmapsto A = \sum L u_\sigma$, $b_{\sigma,\tau} \longmapsto B = \sum L v_\sigma$ so that $a_{\sigma,\tau} \cdot b_{\sigma,\tau} \longmapsto A \otimes_K B = \sum L w_\sigma$ in the notations of Remark 3.3.1 . θ is therefore a group homomorphism. Also by Remark 3.2.3 , we have shown that θ is injective. We have therefore to show now that θ is surjective. Let $\{A\} \in B_{L/K}$. Then by Proposition 2.2.1 , $\exists$ $B \sim A$, $B \supset L$ and $[B : K] = [L : K]^2$. Let $\sigma \in \mathcal{G}_{L/K}$. Then σ defines a K-automorphism $\sigma : L \to L$. By Skolem-Noether's Theorem $\exists$ u_σ an invertible element of B such that $u_\sigma x u_\sigma^{-1} = \sigma(x)$ $\forall$ $x \in L$.

We will show that $\sum L u_\sigma$ which is a sum of subspaces of B , $(u_\sigma \in B)$, is a direct sum. For otherwise choose a relation of the type $x = a_{\sigma_1} u_{\sigma_1} + \ldots + a_{\sigma_t} u_{\sigma_t} = 0$ with t minimal. Clearly $t > 1$ since u_{σ_1} is a unit. Choose $b \in L$

such that $\sigma_1(b) \neq \sigma_2(b)$. Then $\sigma_1(b)x - xb_1$ is zero and of shorter length than x . Contradiction. Since $\sum Lu_\sigma$ is a direct sum, $[\sum Lu_\sigma : K] = [L : K]^2$; also $[B : K] = [L : K]^2$ and so since both have K-dimension $[L : K]^2$ we get $\sum Lu_\sigma = B$.

Let now $a \in L$. Claim that $u_\sigma u_\tau u_{\sigma\tau}^{-1} a = a u_\sigma u_\tau u_{\sigma\tau}^{-1}$. The R.H.S. $= u_\sigma \sigma^{-1}(a) u_\tau u_{\sigma\tau}^{-1} = u_\sigma u_\tau (\tau^{-1}\sigma^{-1}(a)) u_{\sigma\tau}^{-1}$ by (4) of Remark 3.3.4 following the Proposition. Therefore the R.H.S. $= u_\sigma u_\tau u_{\sigma\tau}^{-1} a =$ L.H.S. (Since $u_{\sigma\tau}^{-1} a = (\sigma\tau)^{-1} a u_{\sigma\tau}^{-1}$ implies $a = u_{\sigma\tau}((\sigma\tau)^{-1}a)u_{\sigma\tau}^{-1} \Rightarrow u_{\sigma\tau}^{-1}a = ((\sigma\tau)^{-1}a)u_{\sigma\tau}^{-1}$) . Hence $u_\sigma u_\tau u_{\sigma\tau}^{-1}$ is in the commutant of L in B. But the commutant of L in B is itself since $[B : K] = [L : K]^2$. Therefore $u_\sigma u_\tau u_{\sigma\tau}^{-1} \in L^*$. Let $u_\sigma u_\tau u_{\sigma\tau}^{-1} = a_{\sigma,\tau} \in L^*$. Then $u_\sigma u_\tau = a_{\sigma,\tau} u_{\sigma\tau}$. Since B is an associative ring, $(u_\sigma u_\tau)u_\rho = u_\sigma(u_\tau u_\rho)$. This gives that $a_{\sigma,\tau}$ is a 2-cocycle. The algebra $\sum Lu_\sigma$ actually corresponds to the algebra defined by the cocycle $a_{\sigma,\tau}$. This shows the required surjectivity. Hence the Proposition. #

Remark 3.3.4 : In the Proposition, u_σ is an invertible element of B such that $u_\sigma x u_\sigma^{-1} = \sigma(x) \quad \forall\, x \in L$ ---(*) . $\Rightarrow u_\sigma x = \sigma(x) u_\sigma \quad \forall\, x \in L$ ---(1) . Putting $x = \sigma^{-1}(y)$ in (*), we get $u_\sigma \sigma^{-1}(y) u_\sigma^{-1} = \sigma(\sigma^{-1}(y)) = y$. Therefore $\sigma^{-1}(y) = u_\sigma^{-1} y u_\sigma \quad \forall\, y \in L$, or, writing x for y we get $u_\sigma^{-1} x u_\sigma = \sigma^{-1}(x) \quad \forall\, x \in L$ ---(2) . That is $u_\sigma^{-1} x = \sigma^{-1}(x) u_\sigma^{-1}$ ---(3) . We want to prove that $\sigma^{-1}(a) u_\tau = u_\tau((\sigma\tau)^{-1}a)$, i.e. $u_\tau^{-1}\sigma^{-1}(a)u_\tau = (\sigma\tau)^{-1}a$. Putting $x = \sigma^{-1}(a)$

and $\sigma = \tau$, we get from (2), $u_\tau^{-1}\,\sigma^{-1}(a)u_\tau = {}^{-1}_{\tau}({}^{-1}_{\sigma}(a))$ $= (\sigma\tau)^{-1}a$ ---(4) .

We have so far shown that $B_K = \bigcup B_{L/K}$ where L/K is a finite Galois Extension, and that $B_{L/K} \simeq H^2(\mathcal{G}_{L/K}, L^*)$ if L/K is a finite Galois Extension. Finally, we require the following :

<u>Lemma 3.3.2</u> : Suppose I is an inductive set. Let $\forall\, i \in I$, A_i be some set. For $i < j$ let $f_{ij} : A_i \longrightarrow A_j$ be given maps making $\{A_i\}_{i \in I}$ an inductive family. Assume that the f_{ij}'s are injective maps. Then i) the canonical map say $f_i : A_i \longrightarrow \varinjlim A_i$ is injective and ii) if we identify A_i with a subset of $\varinjlim A_i$ through f_i, then $\varinjlim A_i = \bigcup A_i$.

<u>Proof</u> : Suppose for $x, y \in A_i$, we have $f_i(x) = f_i(y)$. Then for j large enough, $f_{ij}(x) = f_{ij}(y)$. Since f_{ij} is 1-1, this implies $x = y$. Hence f_i is 1-1 and this proves i). The proof of ii) is trivial. Consider $f_i : A_i \to \frac{\bigcup A_i \times \{i\}}{\sim}$ such that $a_i \mapsto (\overline{a_i, i})$. Then $f_i(A_i) \subset \frac{\bigcup A_i \times \{i\}}{\sim}$ and also considering $\frac{\bigcup A_i \times \{i\}}{\sim} \hookrightarrow f_i(A_i)$ such that $(\overline{x_i, i}) \mapsto f_i(x_i) = (\overline{x_i, i})$ we get $\frac{\bigcup A_i \times \{i\}}{\sim} \subset \bigcup f_i(A_i)$. Therefore $\varinjlim A_i = \frac{\bigcup A_i \times \{i\}}{\sim} = \bigcup f_i(A_i)$ and thus upto identification of A_i with $f_i(A_i)$, we conclude that $\varinjlim A_i = \bigcup A_i$. #

<u>Theorem 3.3.3</u> : $B_K \simeq H^2_{\text{prof}}\left(\mathcal{G}_{K_S/K}, K_S^*\right)$.

<u>Proof</u> : Let $K \subset L \subset M$ be a tower of finite extension of K

such that L/K and M/K are both Galois Extensions. Then from the following commutative diagram

$$\begin{array}{ccc} H^2(g_{L/K}, L^*) & \xrightarrow{\text{inflation map}} & H^2(g_{M/K}, M^*) \\ \wr & & \wr \\ B_{L/K} & \xrightarrow{\exists \text{ a natural inclusion}} & B_{M/K} \end{array}$$

we get that the inflation maps $H^2(g_{L/K}, L^*) \to H^2(g_{M/K}, M^*)$ are 1-1. Notice that $B_{L/K} \to B_{M/K}$ is an inclusion because $A \otimes_K L = A \otimes_K M \otimes_M L = M_n(M) \otimes_M L = M_n(L)$, where $A \otimes_K M \cong M_n(M)$.

By the Lemma 3.3.2, we can identify $H^2(g_{L/K}, L^*)$ as a subgroup of $H^2_{prof}\left(g_{K_S/K}, K_S^*\right)$, and then $H^2_{prof}\left(g_{K_S/K}, K_S^*\right) = \bigcup_{L/K} H^2(g_{L/K}, L^*)$. Now $B_K = \bigcup B_{L/K}$, L/K finite Galois, and $B_{L/K} = H^2(g_{L/K}, L^*)$ after this identification. Therefore $B_K = \bigcup B_{L/K} = \bigcup_{L/K} H^2(g_{L/K}, L^*)$, i.e. $B_K = H^2_{prof}\left(g_{K_S/K}, K_S^*\right)$. Hence the theorem. #

****

CHAPTER IV

***

COMPUTATION OF BRAUER GROUPS

In this chapter we compute the Brauer Grpups of $\mathbb{R}, \mathbb{C}$ and that of a finite field. We also show that the Brauer Group of a field is a torsion group. We require the following

<u>Proposition 4.1.1</u> : Let L/K be a finite cyclic field extension. Then $B_{L/K} = K^*/N^*_{L/K}$ where $N^*_{L/K} = \{ N_{L/K}\, x : x \in L^* \}$.

<u>Proof</u> : Let σ be a generator of $\mathcal{G}_{L/K}$, the Galois group of L over K. For $a \in K^*$ we define a cyclic algebra denoted by $[L/K, \sigma, a]$ as follows : Let u be an indeterminate over L. Consider the vector space over L, namely $\sum_{i=0}^{n-1} Lu^i$ where $n = [L : K]$. We make it into a K-algebra by the following rules :

$$\left.\begin{aligned} ux &= \sigma(x)u \quad \text{for} \quad x \in L^* \\ \text{and} \quad u^i u^j &= u^{i+j} \quad \text{if} \quad i+j < n \\ &= a u^{i+j-n} \quad \text{if} \quad i+j \geq n, \\ \text{for all} \quad & i,j,\ 0 \leq i,j \leq n-1 \end{aligned}\right| \quad \text{----(1)}$$

By earlier theory $[L/K, \sigma, a]$ is a Central Simple K-algebra. Define now $\eta : K^* \to B_{L/K}$ as $\eta(x) = [L/K, \sigma, x]$ for any $x \in K^*$. We claim that (i) η is a group homomorphism, (ii) η is surjective and (iii) Kernel $\eta = N_{L/K} L^*$. We proceed to prove these three in their respective orders.

(i) η is a group homomorphism : The cocycle for $[L/K, \sigma, x]$ is $a_{\sigma^i, \sigma^j} = 1$ if $i+j < n$ and $a_{\sigma^i, \sigma^j} = x$ if $i+j \geq n$. So

the cocycle for $[L/K,\sigma,\chi] \otimes [L/K,\sigma,y]$ is

$c_{\sigma^i,\sigma^j} = 1$ if $i+j < n$
$= \chi y$ if $i+j \geq n$ ——(2), by an earlier theory.

Also the cocycle for $[L/K,\sigma,\chi y]$ is given by ——(2) above. Hence $[L/K,\sigma,\chi] \otimes [L/K,\sigma,y] \simeq [L/K,\sigma,\chi y]$. This shows that η is a group homomorphism.

(ii) η is surjective : Let A be a Central Simple K-algebra split by L. Let a_{σ^i,σ^j} be a cocycle corresponding to A, i.e. $A = \sum L u_{\sigma^i}$ and $u_{\sigma^i} u_{\sigma^j} = a_{\sigma^i,\sigma^j} u_{\sigma^{i+j}}$. Let $\chi = \prod_{i=1}^{n-1} a_{\sigma^i,\sigma}$. We will show that $\chi \in K^*$ and that $A \simeq [L/K,\sigma,\chi]$. This will show the required surjectivity. Computing, we have $u_\sigma^2 = u_\sigma u_\sigma = a_{\sigma,\sigma} u_{\sigma^2}$, $u_\sigma^3 = u_\sigma^2 u_\sigma = a_{\sigma,\sigma} u_{\sigma^2} u_\sigma$ $=$
$= a_{\sigma,\sigma} a_{\sigma^2,\sigma} u_{\sigma^3}$,.....,....,
finally $u_\sigma^n = \left(\prod_{i=1}^{n-1} a_{\sigma^i,\sigma}\right) u_{\sigma^n} = \chi u_1 = \chi$, ——(3)
since $u_1 = 1$ and $\sigma^n = 1$.

We claim that u_σ^n belongs to the centre, namely K, of the algebra $\sum L u_{\sigma^i}$. We have only to show that $u_\sigma^n u_{\sigma^i} = u_{\sigma^i} u_\sigma^n$. We have, $u_{\sigma^i} u_\sigma = a_{\sigma^i,\sigma} u_{\sigma^{i+1}}$, $u_{\sigma^i} u_\sigma^2 = a_{\sigma^i,\sigma} u_{\sigma^{i+1}} u_\sigma =$
$a_{\sigma^i,\sigma} a_{\sigma^{i+1},\sigma} u_{\sigma^{i+2}}$ ...., and finally $u_{\sigma^i} u_\sigma^n = \left(\prod_{j=0}^{n-1} a_{\sigma^{i+j},\sigma}\right) u_{\sigma^{i+n}}$
$= \left(\prod_{j=0}^{n-1} a_{\sigma^{i+j},\sigma}\right) u_{\sigma^i} = \chi u_{\sigma^i} = u_\sigma^n u_{\sigma^i}$. [Here $a_{\sigma^i,\sigma} \cdots a_{\sigma^{i+n-1},\sigma}$
$= a_{\sigma,\sigma} a_{\sigma^2,\sigma} \cdots a_{\sigma^{n-1},\sigma}$ for if $\chi' = a_{\sigma,\sigma} a_{\sigma^2,\sigma} \cdots a_{\sigma^{n-1},\sigma}$ then since $a_{1,\sigma} = 1 \ \forall \sigma$, we can write $\chi' = a_{1,\sigma} a_{\sigma,\sigma} \cdots a_{\sigma^{n-1},\sigma}$
i.e. $\chi' = \prod_{\tau \in g_{L/K}} a_{\tau,\sigma}$ = the L.H.S. of the above, since

$\sigma^i, \sigma^{i+1}, \ldots, \sigma^{i+n-1}$ are just a permutation of all the elements of $\{L/K\}$. Also for any $\lambda \in L$, using the fact that $u_\sigma \lambda = \sigma(\lambda) u_\sigma$, we get $\alpha\lambda = u_\sigma^n \lambda = u_\sigma^{n-1} \sigma(\lambda) u_\sigma = \ldots = \sigma^n(\lambda) u_\sigma^n = \lambda u_\sigma^n = \lambda\alpha$ (since $\alpha = u_\sigma^n$ and $\sigma^n = 1$). Hence $\alpha \in K^*$. Consider the algebra $\sum_{i=0}^{n-1} L(u_\sigma)^i$ with multiplication induced from $\sum L u_{\sigma^i}$. Now $u_\sigma^i =$ (an element of L^*) $\times u_{\sigma^i}$ by (3) and so $\{u_\sigma^i\}$ form an L-basis of the algebra $\sum L u_{\sigma^i}$ and thus clearly $\sum L(u_\sigma)^i = \sum L u_{\sigma^i}$ as vector spaces, and hence A is just the algebra $[L/K, \sigma, \alpha]$.

(iii) We now show that kernel $\eta = N_{L/K} L^*$: To do this we will first show that kernel $\eta \supset N_{L/K} L^*$. Take $\alpha \in N_{L/K} L^*$ so that $\exists\ y \in L^*$ with $\alpha = N_{L/K} y$. We have to show that $[L/K, \sigma, \alpha]$ is a matrix algebra over K. For this, we show that $[L/K, \sigma, \alpha] \tilde{\to} [L/K, \sigma, 1]$. We write $[L/K, \sigma, 1]$ in standard form as $\sum L u^i$ with usual multiplication as in (1). Let $v = yu$. Then $v^2 = (yu)^2 = (yu)(yu) = y\sigma(y)uu = y\sigma(y)u^2 = y^{1+\sigma} u^2$, $v^3 = y\sigma(y)\sigma^2(y)u^3 = y^{1+\sigma+\sigma^2} u^3, \ldots, \ldots$, and $v^n = (yu)^n = y^{1+\sigma+\ldots+\sigma^{n-1}} u^n = (N_{L/K} y) u^n = \alpha u^n = \alpha$ since $u^n = 1$. These formulae show that $\sum L u^i = \sum L v^i$. Clearly $\sum L v^i \tilde{\to} [L/K, \sigma, \alpha]$ since $v^n = \alpha$. Hence $[L/K, \sigma, 1] \tilde{\to} [L/K, \sigma, \alpha]$. Conversely, we show that kernel $\eta \subset N_{L/K} L^*$. Suppose $\alpha \in K^*$ such that $[L/K, \sigma, \alpha]$ is a matrix algebra over K. Then the cocycle for $[L/K, \sigma, \alpha]$ must be equivalent to the trivial cocycle, i.e. if a_{σ^i, σ^j} is a cocycle, then $\exists$ $c_{\sigma^i} \in L^*$ such that $a_{\sigma^i, \sigma^j} = c_{\sigma^i} c_{\sigma^j}^{\sigma^i} / c_{\sigma^{i+j}}$ ----(4).

Now $a_{\sigma^i,\sigma^j} = 1$ if $1 + j < n$, and $a_{\sigma^i,\sigma^j} = \alpha$ if $i + j \geq n$. Hence $\prod_{i=0}^{n-1} a_{\sigma^i,\sigma} = \alpha$ and so $\prod_{i=0}^{n-1} c_{\sigma^i} c_{\sigma^j} / c_{\sigma^{i+j}}$ $= c_\sigma c_\sigma^\sigma c_\sigma^{\sigma^2} \ldots c_\sigma^{\sigma^{n-1}} = N_{L/K} c_\sigma$. Thus $\alpha = N_{L/K} c_\sigma$. Finally we get therefore that kernel $\eta = N_{L/K} L^*$.

Hence the proposition. #

We use the above proposition to compute the Brauer Groups of $\mathbb{R}$, $\mathbb{C}$ and that of a finite field.

Remark 4.1.1 : We shall show first that the Brauer Group of the reals is a cyclic group of order 2. Consider $B_{\mathbb{C}/\mathbb{R}}$. Now $\mathbb{C}$ is a cyclic extension of $\mathbb{R}$ of order 2. By Proposition 4.1.1, $B_{\mathbb{C}/\mathbb{R}} = \mathbb{R}^*/N_{\mathbb{C}/\mathbb{R}}\mathbb{C}^*$. We show that $N_{\mathbb{C}/\mathbb{R}}\mathbb{C}^* = \mathbb{R}_+^*$ (i.e. the positive reals). For if $\alpha + iy \in \mathbb{C}^*$ then $N_{\mathbb{C}/\mathbb{R}}(\alpha+iy)$ $= (\alpha+iy)(\alpha-iy) = \alpha^2 + y^2 > 0$, and conversely if $t \in \mathbb{R}_+^*$, then $t = N_{\mathbb{C}/\mathbb{R}}\sqrt{t}$, (positive root). Hence $N_{\mathbb{C}/\mathbb{R}}\mathbb{C}^* = \mathbb{R}_+^*$. Thus $B_{\mathbb{C}/\mathbb{R}} = \mathbb{R}^*/\mathbb{R}_+^*$, which is a cyclic group of order 2. But then since $\mathbb{C}$ is algebraically closed any algebra will be split by $\mathbb{C}$ and therefore $B_{\mathbb{R}} = B_{\mathbb{C}/\mathbb{R}}$. Hence $B_{\mathbb{R}}$ is a cyclic group of order 2.

Remark 4.1.2 : Since $\mathbb{C}$ is algebraically closed, any Central Simple $\mathbb{C}$-algebra is a matrix algebra over $\mathbb{C}$ and hence $B_{\mathbb{C}}$ is trivial.

We shall show presently in this section that if K is a finite field, then B_K is trivial. We require however, the following :

Proposition 4.1.2 : Let K be a finite field and let L be a finite extension of K. Then any element of K is the norm of an element of L.

Proof : The proof of the Proposition requires the following standard result : If G is a finite cyclic group of order n and if d is a divisor of n, then the equation $\chi^d = 1$ has exactly d solutions in G.

For the proof of the proposition, it is enough to prove that any element $\chi \in K^*$ is the norm of an element of L^*. Let $\#K = q$ and $[L : K] = n$. Then $\#L = q^n$. ($\#L$ meaning "cardinality of L"). Let σ be the Frobenius automorphism, i.e. the K-automorphism of L defined by $\sigma a = a^q$ if $a \in L$. Then $\sigma^i a = a^{q^i}$ and hence $N_{L/K}a = a\sigma a\sigma^2 a \ldots \sigma^{n-1} a = a^{q^n-1/q-1}$. Consider now the mapping $N_{L/K} : L^* \to K^*$. Then kernel $N_{L/K} = \{ a \in L^* \text{ such that } a^{\frac{q^n-1}{q-1}} = 1 \}$. Now L^* being a cyclic group, the set $\{ a \in L^* : a^{\frac{q^n-1}{q-1}} = 1 \}$ has cardinality $\frac{q^n-1}{q-1}$ by the result quoted above. Hence

$$[L^* : \text{kernel } N_{L/K}] = \frac{q^n-1}{\frac{q^n-1}{q-1}} = q-1 = \#K^*, \text{ and also}$$

$[L^* : \text{kernel } N_{L/K}] = \#$ of the image of $N_{L/K}$ by an isomorphism theorem. Hence $\#K^* = \#$ of the image of $N_{L/K}$, and both sets being finite, we get $K^* =$ the image of $N_{L/K}$. Hence the proposition. #

Remark 4.1.3 : We show now that the Brauer Group of a finite field is trivial : Let K be a finite field and let L be a

finite extension of K. Then L is a cyclic extension of K. By Proposition 4.1.1, $B_{L/K} = K^*/N_{L/K}L^*$, but by Proposition 4.1.2, $K^* = N_{L/K}L^*$ and so $B_{L/K}$ is trivial. Since now $B_K = \bigcup_L B_{L/K}$ (L ranging through all finite Galois Extensions of K), we get B_K is trivial.

Remark 4.1.4 : Using the fact that the Brauer Group of a finite field is trivial, we can prove that any finite division ring is commutative and is thus a field : Let D be a finite division ring and K be the centre of D. Then K is a finite field, and $[D : K] < \infty$ since D is itself finite. Hence $[D] \in B_K$ where $[D]$ is the Brauer equivalence class of D. Since by Remark 4.1.3, B_K is trivial, we get that D is K-isomorphic to a matrix ring over K, say $M_n(K)$. Since D is a division ring, we must have n = 1, i.e. D = K.

We end this chapter by proving that the Brauer Group of a field is a torsion group. We require however the following Lemma 4.1.3 : Let G be a finite group. Let A be a G-module. Let #G = n. Then for any positive integer i, if $y \in H^i(G,A)$, we have $ny = 0$; i.e. n annihilates any co-homology class of positive dimension.

Proof : Let $y_1, y_2, \ldots, y_{i+1}$ be any i+1 elements of G. Let y be represented by an i-nonhomogeneous cocycle f. Then

$$0 = (\partial f)(y_1, y_2, \ldots, y_{i+1}) = y_1 f(y_2, y_3, \ldots, y_i, y_{i+1}) + \sum_{j=1}^{i-1} (-1)^j f(y_1, y_2, \ldots, y_{j-1}, y_j \cdot y_{j+1}, y_{j+2}, \ldots, y_{i+1}) + (-1)^{i+1} f(y_1, y_2, \ldots, y_i).$$

Now take $y_{i+1} = t$ and let t run through all elements of G, keeping $y_1, y_2, \ldots, y_i$ fixed. Adding the resulting equations and writing $g(y_1, y_2, \ldots, y_{i-1}) = \sum_{t \in G} f(y_1, y_2, \ldots, y_{i-1}, t)$, (notation), we get $0 = y_1 g(y_2, y_3, \ldots, y_i) +$

$$\sum_{j=1}^{i-1} (-1)^j g(y_1, y_2, \ldots, y_{j-1}, y_j \cdot y_{j+1}, y_{j+2}, \ldots, y_i) +$$

$$(-1)^i g(y_1, y_2, \ldots, y_{i-1}) + (-1)^{i+1} nf(y_1, y_2, \ldots, y_i) \text{ , i.e.}$$

$$((-1)^i nf)(y_1, y_2, \ldots, y_i) = y_1 g(y_2, y_3, \ldots, y_i) +$$

$$\sum_{j=1}^{i-1} (-1)^j g(y_1, y_2, \ldots, y_{j-1}, y_j \cdot y_{j+1}, \ldots, y_i) +$$

$(-1)^i g(y_1, y_2, \ldots, y_{i-1}) = \partial g(y_1, y_2, \ldots, y_i)$. Hence nf is a coboundary, i.e. $nf = 0$, or $ny = 0$.

Hence the Lemma. #

<u>Proposition 4.1.4</u> : If K is any field, then B_K is a torsion group, i.e. any element of B_K has finite order.

<u>Proof</u> : Let K be a field and let $y \in B_K$. Since $B_K = \bigcup_{L/K} B_{L/K}$, L running through all finite Galois Extensions of K, we get $y \in B_{L/K}$ for some finite Galois Extension L of K. We also know that $B_{L/K} \xrightarrow{\sim} H^2(\mathcal{G}_{L/K}, L^*)$. By Lemma 4.1.3, n annihilates $H^2(\mathcal{G}_{L/K}, L^*)$, i.e. n annihilates y, i.e. $O(y)$ in B_K is a divisor of n, where $n = \#\mathcal{G}_{L/K}$ and so $O(y)$ is finite. #

****

A brief explanation of some notations used in this dissertation :

$<$	is a subgroup of
$\lhd$	is a normal subgroup of
o(G)	order of the group G
O(y)	order of y
$\sim$	'is equivalent to' or 'is related to'
$\xrightarrow{\sim}$	is isomorphic to
$\amalg$	disjoint union
N-homogeneous	Non-homogeneous
L*	the multiplicative group of the field L
L/K	the Galois group of L over K
#L*	cardinality of L*
(r_{ij})	the matrix with entries r_{ij}
$\mathbb{R}$	the field of real numbers
$\mathbb{C}$	the field of complex numbers
$\mathbb{Z}$	the ring of integers
a^{σ}	$\sigma(a)$
$M_n(R)$	the ring of $n \times n$ matrices with coefficients in R
B_K	the Brauer group of the field K
$B_{L/K}$	the kernel of the homomorphism $B_K \longrightarrow B_L$

BIBLIOGRAPHY

[1] Artin and Tate -- Class Field Theory,Benjamin .

[2] Cartan & Eilenberg -- Homological Algebra,Princeton.

[3] M.Deuring -- Algebran,Ergebnirseder Mathematishe Wissenchaften .

[4] J.P.Serre -- Corps Locaux , Hermann .
