

T.R.
GEBZE TECHNICAL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

BRAUER MANIN OBSTRUCTION

OKTAY CESUR
A THESIS SUBMITTED FOR THE DEGREE OF
MASTER OF SCIENCE
DEPARTMENT OF MATHEMATICS

GEBZE

2021

T.R.
GEBZE TECHNICAL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

BRAUER MANIN OBSTRUCTION

OKTAY CESUR
A THESIS SUBMITTED FOR THE DEGREE OF
MASTER OF SCIENCE
DEPARTMENT OF MATHEMATICS

THESIS SUPERVISOR
ASSIST. PROF. DR. ALTAN ERDOĞAN

GEBZE

2021

T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BRAUER MANIN TIKANIKLIĞI

OKTAY CESUR
YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİMDALI

DANIŞMANI
DR. ÖĞR. ÜYESİ ALTAN ERDOĞAN

GEBZE
2021



YÜKSEK LİSANS JÜRİ ONAY FORMU

GTÜ Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 17/07/2020 tarih ve 2020/34 sayılı kararıyla oluşturulan jüri tarafından 16/11/2020 tarihinde tez savunma sınavı yapılan Oktay CESUR' un tez çalışması Matematik Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

JÜRİ

ÜYE

(TEZ DANIŞMANI) : Dr. Öğr. Üyesi Altan ERDOĞAN

ÜYE

: Dr. Öğr. Üyesi Roghayeh HAFEZIEH

ÜYE

: Doç. Dr. Ayberk Zeytin

ONAY

Gebze Teknik Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun

...../...../..... tarih ve/..... sayılı kararı.

ÖZET

Hasse ilkesi sayı teorisinin önemli teoremlerinden biridir. İkinci dereceden Diophantine denklemlerinin rasyonel çözümlerinin varlığı hakkında çıkarımda bulunmamızı sağlar. Ancak, bu yöntem kuadratik formlar dışında çalışmaz. Hasse ilkesinin bu çöküşü bazı durumlar için Brauer-Manin tıkanıklığı ile açıklanabilir. Çalışmamız bunun nasıl gerçekleştiğini açıklamaktadır.

Anahtar Kelimeler: Hasse İlkesi, Brauer Manin Tıkanıklığı, Brauer Grupları, Diophantine Denklemleri, Faktör Kümeleri

SUMMARY

The Hasse principle is one of the important theorems of number theory. It facilitates us to make illation about the existence of rational solutions of quadratic Diophantine equations. However, this method does not work in non-quadratic forms. In some cases, the failure of the Hasse principle can be explained by Brauer-Manin Obstruction. This study explains how this process works.

Keywords: Hasse Principle, Brauer Manin Obstruction, Brauer Group, Diophantine Equations, Factor Sets.

ACKNOWLEDGEMENTS

I would like to thank my advisor Altan Erdoğan for all his support and devotion. I'm grateful to my wife for support and encouraging. I especially thank my little son, although he always sabotages my study time, for increasing my life energy.

TABLE of CONTENTS

	<u>Page</u>
ÖZET	v
SUMMARY	vi
ACKNOWLEDGMENTS	vii
TABLE of CONTENTS	viii
LIST of ABBREVIATIONS and ACRONYMS	x
1. INTRODUCTION	1
2. PRELIMINARIES	3
2.1. p -adic Numbers	3
2.1.1. Building p -adic Numbers	3
2.1.2. Quadratic Forms and The Hasse Principle	7
2.2. Algebraic Preliminaries	14
2.2.1. Modules and Algebras	14
2.2.2. Tensor Product	18
2.2.3. Tensor Products of Algebras Over a Field	20
2.2.4. Quaternion Algebras	23
2.2.5. Extension of Scalars	24
3. THE BRAUER GROUP	26
3.1. Brauer Group of a Field	26
3.2. Double Centralizer Theorem	27
3.3. Brauer Group of a Ring	33
4. FACTOR SETS AND COHOMOLOGY	36
4.1. Factor Sets and Crossed Product Algebras	36
4.2. Factor Sets and Galois Cohomology Groups	40
5. BRAUER - MANIN OBSTRUCTION	46
5.1. Ring Of Adeles	46
5.2. Obstruction	46

5.3. Example	49
6. CONCLUSION	50
REFERENCES	51
BIOGRAPHY	54
APPENDICES	55

LIST of ABBREVIATIONS and ACRONYMS

<u>Abbreviations</u>	<u>Explanations</u>
<u>and Acronyms</u>	
$\mathbb{Z}$	: The Set of Integers
$\mathbb{Q}$	: The Rational Numbers
$\mathbb{Z}_p$	: Set of p-Adic Integers
$\mathbb{Q}_p$	: Set of p-Adic Numbers
$\mathbb{R}$	: The Real Numbers
$Z(G)$	: The Center of The Group G
$M_n(R)$	: The Ring of $n \times n$ Matrices Over The Ring R
$Hom_R(M, N)$	: The set of all R-module homomorphisms from M to N
$End_R(M)$	: The set of all R-module homomorphisms from M to M
$\mathbb{k}^c$	: Algebraic Closure of field $\mathbb{k}$
$\mathbb{K}/\mathbb{k}$	: Field extension of $\mathbb{k}$ to $\mathbb{K}$
$Gal(\mathbb{K}/\mathbb{k})$	: Galois Group for Field extension of $\mathbb{k}$ to $\mathbb{K}$
$[V : \mathbb{k}]$	: dimension of a V as vector space over $\mathbb{k}$
$\mathbb{K}^*$	: Multiplicative Group $\mathbb{K} - \{0\}$ where $\mathbb{K}$ is field
$gcd(a, b)$	: Greatest common divisor of a and b

1. INTRODUCTION

Diophantine equations are one of the most crucial objects of number theory and mathematics. One of the major purposes of algebra is to find the solution sets of these equations. The Hasse principle has an important place in this field.

Finding rational solutions for Diophantine equations is often tougher than finding solutions in real numbers and p -adic numbers. The Hasse principle says that for a quadratic equation if we can find nontrivial solutions in real numbers and p -adic fields for all p , there exists a nontrivial rational solution. Overall, this result is very strong but has been proven only for quadratic forms. Whether it worked in other cases was definitively determined by Selmer's work. [Selmer, 1951]

After the precise collapse of the Hasse principle outside of the quadratic forms, most mathematicians focused on the reason of failure. In 1971, the reasons were explained by Manin [Manin, 1971]. In order to explain Manin's work, we need some preliminary ideas and concepts. It can be summarized as follows. Let $V(\mathbb{Q})$ and $V(\mathbb{A}_{\mathbb{Q}})$ denote the rational solutions and the adelic solutions of a variety over $\mathbb{Q}$ respectively. Then by the canonical embedding of $\mathbb{Q}$ to $\mathbb{Q}_p$ it is clear that $V(\mathbb{Q}) \subset V(\mathbb{A}_{\mathbb{Q}})$. So in particular if $V(\mathbb{Q}) = \emptyset$ then $V(\mathbb{A}_{\mathbb{Q}}) = \emptyset$. The Hasse principle is just the converse of this simple fact, i.e. for a variety V given by a quadratic form if $V(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$ then $V(\mathbb{Q}) \neq \emptyset$. But it is also well known that the Hasse principle fails in general. Manin has defined a set X such that $V(\mathbb{Q}) \subset X \subset V(\mathbb{A}_{\mathbb{Q}})$. In some cases it can be found as $X = \emptyset$ while $V(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$. Then $V(\mathbb{Q}) = \emptyset$, but the Hasse principle fails.

To define the set X , we will first define Brauer groups. For this, we need the basic properties of the tensor product and central simple algebras. We will also briefly cover the relation between Brauer groups of fields and some Galois cohomology groups. Next, we will need the Brauer groups of the coordinate ring of a given variety. For this, we will define the Brauer group of a commutative ring using Azumaya algebras.

Also, we need to define the adelic points of a variety denoted by $V(\mathbb{A}_{\mathbb{Q}})$ and we will construct the set $X = V(\mathbb{A}_{\mathbb{Q}})^{Br}$ mentioned above as a subset of $V(\mathbb{A}_{\mathbb{Q}})$. We will complete the process of Brauer-Manin obstruction by utilizing a fundamental theorem of class field theory. If for a variety V over $\mathbb{Q}$, $V(\mathbb{A}_{\mathbb{Q}})$ is non-empty, but $V(\mathbb{A}_{\mathbb{Q}})^{Br}$ is

empty then we may say that there is a Brauer-Manin obstruction to the Hasse principle.

It must also be noted that the Brauer-Manin obstruction is not a complete obstruction in the following sense. There are examples of varieties where $V(\mathbb{A}_{\mathbb{Q}})^{Br} = \emptyset$ but $V(\mathbb{Q}) \neq \emptyset$. This is beyond the scope of this thesis but for an example of such varieties, the reader is referred to [Skorobogatov, 1999].

2. PRELIMINARIES

2.1. p -adic Numbers

In this section, we will only give definitions and basic facts about p -adic numbers without proofs. For details, the reader is referred to Section 1 of [Borevich and Shafarevich, 1986].

2.1.1. Building p -adic Numbers

Two different methods can be used in the construction of p -adic numbers. The first way is taking the completion of $\mathbb{Q}$ with respect to p -adic metric. The second way which will be used here is based on the basic modular arithmetic process. We start with constructing p -adic integers.

Definition 2.1: (p -adic Integers) Let $\alpha = \{x_k\}_{k=1}^{\infty}$ be a sequence of integers and p be a prime number. α is called a p -adic integer if it satisfies the following two conditions:

- i) $x_{k+1} \equiv x_k \pmod{p^k}$ for each k .
- ii) Two sequences $\{x_k\}$ and $\{y_k\}$ determine the same p -adic integer if and only if $x_k \equiv y_k \pmod{p^k}$ for each k .

Set of p -adic integers is denoted by $\mathbb{Z}_p$.

Theorem 2.1: Let the addition and multiplication of p -adic integers denoted by $+$ and $\cdot$ respectively be defined as

$$\{x_k\} + \{y_k\} = \{x_k + y_k\} \quad (2.1)$$

$$\{x_k\} \cdot \{y_k\} = \{x_k y_k\} \quad (2.2)$$

for any $\{x_k\}, \{y_k\} \in \mathbb{Z}_p$. Then $(\mathbb{Z}_p, +, \cdot)$ is a commutative ring with identity.

Proof [Borevich and Shafarevich, 1986] [p: 21] ■

Example 2.1: Consider the equation $x^2 - 2 = 0$. There are two distinct solutions of this equation modulo 7. Let's take the solution $x_1 \equiv 4$. Now for each integer $k \geq 2$,

we can find x_k such that

$$x_k^2 \equiv 2 \pmod{7^k} \quad (2.3)$$

$$x_{k+1} \equiv x_k + a_k 7^k \pmod{7^{k+1}} \quad (2.4)$$

for some integer a_k for which $0 \leq a_k \leq 6$. For instance, we can see that

$$\begin{aligned} x_2^2 &\equiv (4 + a_1 7)^2 \equiv 2 \pmod{7^2} \\ \implies 16 + 56a_1 + 49a_1^2 &\equiv 2 \pmod{7^2} \\ \implies 14 + 7a_1 &\equiv 0 \pmod{7^2} \\ \implies a_1 &\equiv 5 \pmod{7} \end{aligned} \quad (2.5)$$

So we find $x_2 \equiv 4 + 5 \cdot 7 \pmod{7^2}$. Continuing in this way, we obtain

$$\begin{aligned} x_3 &\equiv 4 + 5 \cdot 7 + 4 \cdot 7^2 \pmod{7^3} \\ x_4 &\equiv 4 + 5 \cdot 7 + 4 \cdot 7^2 + 0 \cdot 7^3 \pmod{7^4} \end{aligned} \quad (2.6)$$

$$x_5 \equiv 4 + 5 \cdot 7 + 4 \cdot 7^2 + 0 \cdot 7^3 + 5 \cdot 7^4 \pmod{7^5}$$

Therefore $\alpha = \{4, 39, 235, 235, 12240, \dots\}$ is a solution of the equation $x^2 - 2 = 0$ in $\mathbb{Z}_7$. In a similar way if we start with $x_1 \equiv 3 \pmod{7}$ we obtain another solution in $\mathbb{Z}_7$.

It is also easy to see that the map

$$\begin{aligned} \mathbb{Z} &\rightarrow \mathbb{Z}_p \\ \alpha &\mapsto \{\alpha, \alpha, \alpha, \dots\} \end{aligned} \quad (2.7)$$

is a one-to-one ring homomorphism. Since the additive and multiplicative identities of $\mathbb{Z}_p$ are $\{0, 0, \dots\}$ and $\{1, 1, \dots\}$, we obtain the following result.

Corollary 2.1: $\mathbb{Z}_p$ has a subring that is isomorphic to $\mathbb{Z}$.

Now we give some well-known properties of p -adic integers. For p -adic integers β and α , we say that β divides α if there exists a p -adic integer γ such that $\alpha = \gamma \cdot \beta$.

Proposition 2.1: Let $\alpha = \{x_0, x_1, \dots\}$ be a p -adic integer and $U(\mathbb{Z}_p)$ be the set of units in $\mathbb{Z}_p$. Then $\alpha \in U(\mathbb{Z}_p)$ if and only if $x_0 \not\equiv 0 \pmod{p}$

Proof [Borevich and Shafarevich, 1986][p: 22] ■

Theorem 2.2: Let α be a nonzero p -adic integer. Then there exist a unique p -adic unit ε and a unique non-negative integer n such that

$$\alpha = p^n \varepsilon \quad (2.8)$$

Proof [Borevich and Shafarevich, 1986][p: 22-23] ■

Corollary 2.2: The p -adic integer $\alpha = \{x_0, x_1, \dots\}$ is divisible by p^n if and only if $x_k \equiv 0 \pmod{p^{k+1}}$ for all $k = 0, 1, 2, \dots, n-1$.

Proof [Borevich and Shafarevich, 1986][p: 23] ■

Let α and β be p -adic integers. If $\alpha - \beta$ is divisible by p^n then we may shortly write $\alpha \equiv \beta \pmod{p^n}$.

Example 2.2:

1. The 7-adic integer $\alpha = \{4, 39, 235, 235, 12240, \dots\}$ found in Example 2.1 is a 7-adic unit. Let $\beta = \alpha + 10$. So $\beta = \{14, 49, 245, 245, 12250, \dots\} = \{0, 0, 245, 245, 12250, \dots\}$ is not 7-adic unit. Also

$$\beta = \{0, 0, 245, 245, 12250, \dots\} = 7^2 \{1, 1, 5, 5, 250, \dots\} \quad (2.9)$$

2. Consider 125 as a 5-adic integer and denoted it by γ . Then

$$\gamma = \{0, 0, 0, 125, 125, \dots\} = 5^3 \{1, 1, 1, 1, 1, \dots\} \quad (2.10)$$

Corollary 2.3: $\mathbb{Z}_p$ is an integral domain.

Proof [Borevich and Shafarevich, 1986][p: 23] ■

Since $\mathbb{Z}_p$ is an integral domain, we can talk about its field of fractions denoted by $\mathbb{Q}_p$.

Definition 2.2: The field of fractions of $\mathbb{Z}_p$ is also called as the field of p -adic numbers and is denoted by $\mathbb{Q}_p$. An element of $\mathbb{Q}_p$ is called a p -adic number. We also set $\mathbb{Q}_\infty = \mathbb{R}$.

We can represent p -adic numbers in a more useful form.

Theorem 2.3: Any p -adic number can be written in the form $\frac{\alpha}{p^k}$ for some p -adic integer α and natural number k , i.e. $\mathbb{Q}_p = \left\{ \frac{\alpha}{p^k} : \alpha \in \mathbb{Z}_p, k \in \mathbb{N} \right\}$. Moreover $\frac{\alpha}{p^m} = \frac{\beta}{p^n}$ in $\mathbb{Q}_p$ if and only if $\alpha p^n = \beta p^m$ in $\mathbb{Z}_p$.

Proof First note that for any $\alpha \in \mathbb{Z}_p$ and $k \in \mathbb{N}$, α/p^k is a p -adic number. Conversely for any $x \in \mathbb{Q}_p$, take any $\alpha, \beta \in \mathbb{Z}_p$ such that

$$x = \frac{\alpha}{\beta} \tag{2.11}$$

Then by Theorem 2.2 we can uniquely write $\beta = \varepsilon p^n$ where ε is a p -adic unit and n is natural number. But $\alpha' = \frac{\alpha}{\varepsilon}$ is also a p -adic integer, so $x = \frac{\alpha'}{p^n}$. Also for any other $\alpha_1, \beta_1 \in \mathbb{Z}_p$ with

$$x = \frac{\alpha}{\beta} = \frac{\alpha_1}{\beta_1} \tag{2.12}$$

If we write $\beta_1 = \varepsilon_1 p^{n'}$ for some p -adic unit ε_1 and natural number n' , we obtain

$$\varepsilon_1 p^{n'} \alpha = \varepsilon p^n \alpha_1. \tag{2.13}$$

So we obtain

$$\frac{(\alpha_1/\varepsilon_1)}{p^{n'}} = \frac{(\alpha/\varepsilon)}{p^n} \tag{2.14}$$

which implies that representation of x in the form α/p^k is well-defined. This proves that

$$\mathbb{Q}_p := \left\{ \frac{\alpha}{p^k} : \alpha \in \mathbb{Z}_p, k \in \mathbb{N} \right\} \quad (2.15)$$

The second part follows by definition of the field of fractions. ■

Indeed we can also extend Theorem 2.2 to obtain a useful representation of p -adic numbers.

Theorem 2.4: Let α be a nonzero p -adic number. Then there exist a unique p -adic unit ε and a unique integer n such that

$$\alpha = p^n \varepsilon \quad (2.16)$$

Proof [Borevich and Shafarevich, 1986][p: 26] ■

2.1.2. Quadratic Forms and The Hasse Principle

Definition 2.3: (Quadratic Form) Let $f(x_1, x_2, \dots, x_n)$ be a polynomial. We say that f is a quadratic form if it is a homogeneous polynomial of degree 2.

Example 2.3: $g(x, y) = x^2 + y^2$ and $f(x, y, z) = 3x^2 + 2xy + z^2$ are quadratic forms.

Definition 2.4: (Quadratic Residue) An integer a is called a quadratic residue modulo n if there exists an integer x such that $x^2 \equiv a \pmod{n}$.

Example 2.4: $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$ and $2^2 \equiv 6^2 \equiv 4 \pmod{8}$. Therefore 1 and 4 are quadratic residues $\pmod{8}$.

Definition 2.5: (Legendre Symbol) Let p be an odd prime number and m be an integer. The Legendre symbol of m , denoted by $\left(\frac{m}{p}\right)$, is defined as follows:

$$\left(\frac{m}{p}\right) = \begin{cases} +1 & \text{if } m \text{ is a quadratic residue } \pmod{p} \\ -1 & \text{if } m \text{ is not a quadratic residue } \pmod{p} \\ 0 & m \equiv 0 \pmod{p} \end{cases} \quad (2.17)$$

Example 2.5: $1^2 \equiv 6^2 \equiv 1 \pmod{7}$, $2^2 \equiv 5^2 \equiv 4 \pmod{7}$ and $3^2 \equiv 4^2 \equiv 2 \pmod{7}$. Therefore 1, 2 and 4 are quadratic residues $\pmod{7}$. Also $\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$, $\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$ and $\left(\frac{7}{7}\right) = 0$

Theorem 2.5: Let p, q be different odd primes and m, n be integers. Then

$$i) \left(\frac{m}{p}\right) \equiv m^{\frac{p-1}{2}} \pmod{p} \quad (\text{Euler's criterion})$$

$$ii) \left(\frac{m}{p}\right) = \left(\frac{n}{p}\right) \text{ if } m \equiv n \pmod{p}$$

$$iii) \left(\frac{m \cdot n}{p}\right) = \left(\frac{m}{p}\right) \left(\frac{n}{p}\right)$$

$$iv) \left(\frac{2}{p}\right) = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$$

$$v) \left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \quad (\text{the quadratic reciprocity law})$$

Proof [Niven et al, 1991] [p: 132 and 137] ■

Example 2.6: We check whether 1189 is a quadratic residue $\pmod{1223}$ or not. Note that 1223 is a prime number, so we can use Theorem 2.5. By the part iii) of Theorem 2.5 we see that

$$\left(\frac{1189}{1223}\right) = \left(\frac{29}{1223}\right) \left(\frac{41}{1223}\right) \quad (2.18)$$

Since 29 and 41 are primes we can use the part v) (the quadratic reciprocity law) of the theorem;

$$\left(\frac{29}{1223}\right) \cdot \left(\frac{1223}{29}\right) = (-1)^{\frac{(23-1)(1223-1)}{4}} = 1 \quad (2.19)$$

But $\left(\frac{1223}{29}\right) = \left(\frac{5}{29}\right) \equiv 5^{\frac{(29-1)}{2}} \equiv 1 \pmod{29}$ where we use the part ii) and the part i) of the above theorem respectively. So we obtain that $\left(\frac{29}{1223}\right) = 1$. A similar computation gives that $\left(\frac{41}{1223}\right) = -1$. Then

$$\left(\frac{1189}{1223}\right) = \left(\frac{29}{1223}\right) \cdot \left(\frac{41}{1223}\right) = 1(-1) = -1 \quad (2.20)$$

Therefore 1189 is not a quadratic residue (mod 1223).

The Legendre symbol can be extended to p -adic units as we outline below. But first, we give some results about the existence of square roots of p -adic units.

Theorem 2.6: Let p be an odd prime and $\varepsilon = \{x_1, x_2, \dots\}$ be a p -adic unit. Then ε is a square in $\mathbb{Q}_p$ if and only if x_1 is a quadratic residue modulo p .

Proof [Borevich and Shafarevich, 1986][p: 48] ■

Theorem 2.7: A 2-adic unit ε is a square in $\mathbb{Q}_2$ if and only if $\varepsilon \equiv 1 \pmod{8}$.

Proof [Borevich and Shafarevich, 1986][p: 49] ■

Definition 2.6: Let ε be a p -adic unit. The Legendre symbol of ε is defined as

$$\left(\frac{\varepsilon}{p}\right) = \begin{cases} +1 & \text{if } \varepsilon \text{ is a square in } \mathbb{Z}_p. \\ -1 & \text{if } \varepsilon \text{ is not a square in } \mathbb{Z}_p. \end{cases} \quad (2.21)$$

In particular if p is an odd prime and $\varepsilon = \{x_1, x_2, \dots\}$ is a p -adic unit, then by Theorem 2.6 we see that

$$\left(\frac{\varepsilon}{p}\right) = \left(\frac{x_1}{p}\right) \quad (2.22)$$

This allows us to carry out some parts of Theorem 2.5 to Legendre symbol of p -adic units.

Theorem 2.8: Let ε and ε' be p -adic units where p is an odd prime. Then

- i) $\left(\frac{\varepsilon}{p}\right) = \left(\frac{\varepsilon'}{p}\right)$ if and only if $\varepsilon \equiv \varepsilon' \pmod{p}$.
- ii) $\left(\frac{\varepsilon\varepsilon'}{p}\right) = \left(\frac{\varepsilon}{p}\right) \left(\frac{\varepsilon'}{p}\right)$

Note that for $p = 2$ slight modifications are required to relate the Legendre symbol of p -adic units and of integers. Now we can characterize the p -adic integers which have square roots in $\mathbb{Z}_p$.

Theorem 2.9: Let p be a prime, $\varepsilon = \{x_1, x_2, \dots\}$ be a p -adic unit and $\alpha = p^m\varepsilon$ be a p -adic number.

i) Let $p \geq 3$. Then α is a square in $\mathbb{Q}_p$ if and only if $\left(\frac{\varepsilon}{p}\right) = 1$ and m is even.

ii) α is a square in $\mathbb{Q}_2$ if and only if $\varepsilon \equiv 1 \pmod{8}$ and m is even.

Proof Let $\alpha = p^m \varsigma$ where ς is a p -adic unit. If α is the square of a p -adic number $\beta = p^n \varepsilon$ then $\alpha = p^{2n} \varepsilon^2$. So by Theorem 2.4 we must have that $m = 2n$ and $\varsigma = \varepsilon^2$. The converse is obvious. ■

The above theorem also indicates why the Legendre symbol is only defined for p -adic units. For example let $\alpha = p\varepsilon$ and $\beta = p\varepsilon'$ where ε and ε' are p -adic units with

$$\left(\frac{\varepsilon}{p}\right) = 1, \quad \left(\frac{\varepsilon'}{p}\right) = -1 \quad (2.23)$$

But obviously $\alpha \equiv \beta \equiv 0 \pmod{p}$. Also both α and β are non-squares. But $\alpha\beta = p^2\varepsilon\varepsilon'$ which is also a non-square. So if we intent to define the Legendre symbol of a non-unit p -adic integer in the same manner, Theorem 2.8 which is a core fact for us would fail.

Definition 2.7: (The Hilbert Symbol) Let $\mathbb{k}$ be a field and $\alpha, \beta \in \mathbb{k}^*$. The Hilbert symbol of α and β denoted by $(\alpha, \beta)_{\mathbb{k}}$ is defined as

$$(\alpha, \beta)_{\mathbb{k}} = \begin{cases} +1, & \text{if } \alpha x^2 + \beta y^2 = z^2 \text{ has a nontrivial solution } (x, y, z) \text{ in } \mathbb{k}^3. \\ -1, & \text{otherwise.} \end{cases} \quad (2.24)$$

If $k = \mathbb{Q}_p$ we may denote the Hilbert symbol of α and β by $(\alpha, \beta)_p$. Similarly if $k = \mathbb{R}$ then we may use $(\alpha, \beta)_{\infty}$.

Example 2.7:

- i) $(1, 1)_{\mathbb{Q}} = 1$ since $x^2 + y^2 = z^2$ has a nontrivial rational solution, e.g $(x, y, z) = (3, 4, 5)$.
- ii) $(-1, -1)_{\mathbb{R}} = -1$ since $-x^2 - y^2 = z^2$ has no solution in $\mathbb{R}$ other than $(x, y, z) = (0, 0, 0)$.

Theorem 2.10: Let p be a prime number and $a, b, c \in \mathbb{Q}_p$, then

$$i) (a, b)_p = (b, a)_p$$

$$ii) (a, bc)_p = (a, b)_p (a, c)_p$$

$$iii) (a, -a)_p = 1$$

$$iv) (a, 1 - a)_p = 1 \text{ if } a \neq 1$$

Proof Part i) follows by definition. Note that $(x, y, z) = (\alpha, \alpha, 0)$ satisfies $ax^2 - ay^2 = z^2$ for any $\alpha \in \mathbb{Q}_p$ which proves Part iii) Similarly the solution $(x, y, z) = (\alpha, \alpha, \alpha)$ of $ax^2 + (1 - a)y^2 = z^2$ proves Part iv) The reader is referred to I.6.3 of [Borevich and Shafarevich, 1986] for the proof of Part ii) ■

The Hilbert and Legendre symbols are closely related to each other. The next theorem clarifies this relation, but first we set the following notation. For any odd integer a , let

$$\epsilon(a) = \frac{a-1}{2}, \quad \omega(a) = \frac{a^2-1}{8} \quad (2.25)$$

Note that $\epsilon(a)$ and $\omega(a)$ are integers.

Theorem 2.11: (Calculating Hilbert Symbol Via Legendre Symbol) Let p be a prime, and m, n, u and v be integers such that $p \nmid uv$. Let $a = p^m u$ and $b = p^n v$. Then

$$(a, b)_p = \begin{cases} (-1)^{\epsilon(p)mn} \left(\frac{u}{p}\right)^n \left(\frac{v}{p}\right)^m & \text{if } p \neq 2. \\ (-1)^{\epsilon(u)\epsilon(v)+m\omega(v)+n\omega(u)} & \text{if } p = 2. \end{cases} \quad (2.26)$$

Proof [Serre, 2012][p: 20-22] ■

Theorem 2.12: (Hasse-Minkowski Theorem or Hasse Principle) Let f be a quadratic form in $\mathbb{Q}[x_1, x_2, \dots, x_n]$. The equation $f(x_1, \dots, x_n) = 0$ has a solution in $\mathbb{Q}$ if and only if it has a solution in $\mathbb{R}$ and $\mathbb{Q}_p$ for all p .

Proof [Borevich and Shafarevich, 1986][p: 61-62] ■

We finish this section with an example where the Hasse Principle for non-quadratic equations fail. But we first need to recall Hensel's lemma.

Theorem 2.13: [Hensel Lemma] Let $f \in \mathbb{Z}[x]$. If $f(a) \equiv 0 \pmod{p^k}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there exists an integer n such that $f(a + np^k) \equiv 0 \pmod{p^{k+1}}$.

Proof [Niven et al, 1991][p: 87] ■

Hensel's lemma allows us to successively find solutions of $f(x) \equiv 0 \pmod{p^k}$ for all $k \geq 1$ provided that we start with a solution $a \pmod{p}$ with $f(a) \equiv 0$ and $f'(a) \not\equiv 0 \pmod{p}$. If we denote the corresponding solutions $\pmod{p^k}$ by $\{x_k\}$ then we obtain a sequence satisfying $x_{k+1} = x_k + tp^k$. So that $\{x_k\}$ is a p -adic integer. Note that this is exactly the way that we constructed an example of a p -adic number in Example 2.1.

Example 2.8: Let $f(x) = x^2 - 2$ and $p = 7$. We take $x_1 = 4$. $f(4) = 16 - 2 \equiv 0 \pmod{7}$ and $f'(4) = 2 \cdot 4 = 8 \not\equiv 0 \pmod{7}$. Then

$$\begin{aligned}
 (n = 2) \quad x_2 &= 4 + 5 \cdot 7 = 39 \\
 (n = 3) \quad x_3 &= 39 + 4 \cdot 7^2 = 235 \\
 (n = 4) \quad x_4 &= 235 + 0 \cdot 7^3 = 235 \\
 (n = 5) \quad x_5 &= 235 + 5 \cdot 7^4 = 12240
 \end{aligned}
 \tag{2.27}$$

Example 2.9: (Failure of the Hasse Principle) The equation $(x^2 - 3)(x^2 + 3)(x^2 + 1)(x^2 - 73) = 0$ has clearly no rational solution but has a real solution, namely $x = \sqrt{3}$. As we outline below it also has a solution in $\mathbb{Q}_p$ for any prime p .

- $p > 3$

$\left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{-3}{p}\right)$ by the Theorem 2.5. Then at least one of $-1, -3$ or 3 is a quadratic residue $\pmod{p}$. So at least one of the congruence $x^2 - 3 \equiv 0$, $x^2 + 1 \equiv 0$ or $x^2 + 3 \equiv 0$ has a solution $\pmod{p}$. In any case the derivative of the polynomial is $2x$, so that the solution satisfies the hypothesis of Hensel's lemma. By successive application of Hensel lemma, we can construct a solution $x_k \pmod{p^k}$ for each $k \geq 1$. So we can construct a p -adic number which is a root of $(x^2 - 3)$, $(x^2 + 3)$ or $(x^2 + 1)$.

- $p = 3$

$\left(\frac{73}{3}\right) = \left(\frac{1}{3}\right) = 1$, so that $f(x) = x^2 - 73 \equiv x^2 - 1 \equiv 0 \pmod{3}$ has a solution. We can choose $x_1 \equiv 1 \pmod{3}$ as a solution. Since $f'(1) \equiv 2 \pmod{3}$, by Hensel's lemma $x^2 - 73 = 0$ has a solution in $\mathbb{Z}_3$.

- $p = 2$

$73 \equiv 1 \pmod{8}$. Then by Theorem 2.9, 73 is a square in $\mathbb{Z}_p$. Hence, $x^2 - 73 = 0$ has a solution in $\mathbb{Z}_2$.

Therefore the Hasse principle fails for this equation.

2.2. Algebraic Preliminaries

This section is devoted to algebraic preliminaries required to build the Brauer-Manin obstruction. First, we give will basic facts about modules that we will need. After defining the tensor product and some of its features, we will continue with the Brauer groups.

2.2.1. Modules and Algebras

By a ring, we always mean a commutative ring with a multiplicative identity unless otherwise specified.

Definition 2.8: Let R be a ring and M be an abelian group. Suppose that we have a map $\mu : R \times M \rightarrow M$ denoted as $(r, m) \mapsto \mu(r, m) = r \cdot m$. M is called a left R -module if the pair (M, μ) satisfies the following conditions:

- i) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$*
- ii) $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$*
- iii) $(r_1 \cdot r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$*

If the conditions are satisfied for the right multiplication, M is called a right R -module. If the conditions are satisfied for two-sided multiplication, M is called an R -module.

Example 2.10: Every abelian group is a $\mathbb{Z}$ -module.

Definition 2.9: Let R be a ring and M be an R -module. Let N be a subgroup of M and X be any subset of M . Also let $r \in R$ and $n \in N$.

- i) N is called a submodule of M if $r \cdot n \in N$ for any $r \in R$ and $n \in N$.*
- ii) The submodule of M spanned by X and denoted by $\langle X \rangle$ is the intersection of all submodules of M which contain X .*

Definition 2.10: Let M, N be R -modules and $f : M \rightarrow N$ be a map. f is called an R -module homomorphism if the following conditions are satisfied for all $m, m' \in M$, and for all $r \in R$.

$$f(m + m') = f(m) + f(m') \quad (2.28)$$

$$f(rm) = r.f(m) \quad (2.29)$$

Also the set of all module homomorphisms from M to N is denoted by $\text{Hom}_R(M, N)$ or by $\text{Hom}(M, N)$ if R is understood.

Note that $\text{Hom}(M, N)$ is also an R -module with the following operations:

$$(f + g)(m) = f(m) + g(m) \text{ for all } m \in M. \quad (2.30)$$

$$(rf)(m) = r.f(m) \text{ for all } m \in M \text{ and for all } r \in R. \quad (2.31)$$

Definition 2.11: Let L and R be rings and M be an abelian group. M is called an $L - R$ -bimodule if the following two conditions hold:

- i) M is both a right R -module and a left L -module.
- ii) $l.(m.r) = (l.m).r$ for all $r \in R, l \in L$ and $m \in M$.

Definition 2.12: Let M be an R -module and X be a nonempty subset of M .

- i) We say that X generates M if for any $m \in M$, there exists finitely many elements $x_1, \dots, x_n \in X$ and $r_1, \dots, r_n \in R$ such that $m = r_1x_1 + r_2x_2 + \dots + r_nx_n$. In this case we also say that X is a generating set of M .
- ii) If M has a finite generating set then M is said to be a finitely generated R -module.
- iii) M is called a free R -module if there is a family of elements $S = \{y_\alpha\}_{\alpha \in I}$ of M such that any element $m \in M$ can be uniquely written as a finite sum $m = \sum_{\alpha \in I} r_\alpha \cdot y_\alpha$ for some $r_\alpha \in R$. In this case we say that S is a basis for the free R -module M .

Example 2.11:

- i) Let R be a commutative ring. The polynomial ring $R[x]$ is a free R -module and the set of $\{x^n : n \in \mathbb{N}\}$ is basis.
- ii) Let k be any field. Every vector space over k is a free k -module.

iii) Consider $\mathbb{Z}/2\mathbb{Z}$ as a $\mathbb{Z}/6\mathbb{Z}$ -module, by the map

$$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}, \quad (2.32)$$

$$(\bar{x}, \bar{y}) \mapsto \bar{x} \cdot \bar{y} = \bar{xy} \quad (2.33)$$

So apparently $\bar{1} \cdot \bar{4} = \bar{0} = \bar{1} \cdot \bar{2}$ which implies that $\mathbb{Z}/2\mathbb{Z}$ is not a free $\mathbb{Z}/6\mathbb{Z}$ -module.

Lemma 2.1: Let M be an R -module and N be a submodule of M . Let X be a nonempty subset of M . We set $(N : X) = (N :_R X) = \{r \in R : rX \subset N\}$. Then

i) $(N : X)$ is an ideal of R .

ii) $(N : X) = (N : \langle X \rangle)$

Proof [Çallialp and Tekir, 2009][p: 116] ■

Definition 2.13: Let M be an R -module and X be a nonempty subset of M . The ideal $(0 : X) = \{r \in R : rX = 0\}$ is called the annihilator of X and denoted by $\text{Ann}(X)$. M is said to be faithful if $\text{Ann}(M) = \langle 0 \rangle$.

Example 2.12: Let n be a positive integer and $M = \mathbb{Z}/n\mathbb{Z}$ considered as a $\mathbb{Z}$ -module. The annihilator of M is $n\mathbb{Z}$, so that M is not a faithful $\mathbb{Z}$ -module. But the $\mathbb{Z}$ -module $\mathbb{Z}[x_1, x_2, \dots, x_n]$ is faithful.

Theorem 2.14: Let M, N and P be R -modules. The following conditions are equivalent.

i) P is a direct summand of a free module over R .

ii) For every R -epimorphism $f : M \rightarrow P$, there exists a homomorphism $g : P \rightarrow M$ such that $fg = 1_P$.

iii) Given an R -homomorphism $h : P \rightarrow N$ and an R -epimorphism $g : M \rightarrow N$ there exists an R -module homomorphism $\tilde{h} : P \rightarrow M$ such that the following diagram commutes:

$$\begin{array}{ccccc} M & \xrightarrow{g} & N & \longrightarrow & 0 \\ & \nwarrow \tilde{h} & \uparrow h & & \\ & & P & & \end{array} \quad (2.34)$$

Proof [Çallıalp and Tekir, 2009][p: 144-145] ■

Definition 2.14: An R -module P is called a projective module if it satisfies one of the equivalent conditions of the Theorem 2.14.

Example 2.13:

- i) By part i) of Theorem 2.14, any free module is projective.
- ii) Let k be a field and $R = k \times k$. So that R is a ring with pointwise addition and multiplication. Let $I = k \times \{0\}$. Note that I is an ideal of R and so is an R -module. Since for example $(1, 0) \cdot (0, 1) = (0, 0)$, we see that I is not a free R -module. But clearly $I \oplus I' = R$ where $I' = \{0\} \times k$, and so by part i) of Theorem 2.14 I is projective.

Definition 2.15: Let M_n be an R -module and $f_n : M_{n-1} \longrightarrow M_n$ be an R -module homomorphism for each $n \geq 1$. The sequence

$$\cdots \longrightarrow M_{n-1} \xrightarrow{f_n} M_n \xrightarrow{f_{n+1}} M_{n+1} \xrightarrow{f_{n+2}} \cdots \quad (2.35)$$

is called an exact sequence if for all $n \geq 0$, we have that $\text{Im}(f_n) = \text{Ker}(f_{n+1})$ where $\text{Im}(f_n)$ and $\text{Ker}(f_{n+1})$ denote the image and kernel of the related maps.

An exact sequence of the form $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ is called a short exact sequence.

It follows by definition that a sequence $0 \rightarrow L \xrightarrow{f} M$ is exact if and only if f is injective. Similarly the sequence $M \xrightarrow{g} N \rightarrow 0$ is exact if and only if g is surjective.

Example 2.14: Let R be a ring and M, N be R -modules. Let $f : M \rightarrow N$ be an R -module homomorphism. We can associate two basic short exact sequences.

$$0 \longrightarrow \text{Ker}(f) \xrightarrow{i} M \xrightarrow{f} \text{Im}(f) \longrightarrow 0 \quad (2.36)$$

$$0 \longrightarrow \text{Im}(f) \xrightarrow{i} N \xrightarrow{\pi} N/\text{Im}(f) \longrightarrow 0 \quad (2.37)$$

where i denotes the relevant inclusion map and π is the canonical surjection.

Definition 2.16: Let R be a ring and $\mathcal{A}$ be a not necessarily commutative ring which is also an R -module.

- i) $\mathcal{A}$ is called an R -algebra if $r.(ab) = (r.a)b = a(r.b)$ for all $r \in R$ and $a, b \in \mathcal{A}$.
- ii) An R -algebra $\mathcal{A}$ is called a division algebra if $\mathcal{A}$ is a division ring.
- iii) An R -algebra $\mathcal{A}$ is called simple if it has no non-trivial two-sided ideal.
- iv) The center of an R -algebra $\mathcal{A}$ is defined as $Z(\mathcal{A}) = \{x \in \mathcal{A} : xa = ax \text{ for all } a \in \mathcal{A}\}$. Also $\mathcal{A}$ is called a central R -algebra if $Z(\mathcal{A}) = R$.
- v) An R -algebra $\mathcal{A}$ is called central simple if it is a central and simple algebra.
- vi) Let $\mathcal{A}$ and S be R -algebras. S is called a subalgebra of $\mathcal{A}$ if $S \subset \mathcal{A}$.

Definition 2.17: The set of all $n \times n$ matrices denoted $M_n(R)$ over a ring R is called a matrix ring with matrix addition and multiplication.

Note that $M_n(R)$ is an R -algebra where $r.\{a_{ij}\} = \{r.a_{ij}\}$ for $r \in R$ and $\{a_{ij}\} \in M_n(R)$ [Farb and Dennis, 2012] [p: 10]

Example 2.15: Let k be a field. Then for any $n \geq 1$, $M_n(k)$ is a central simple k -algebra. [Web 8, 2020] [p: 1]

2.2.2. Tensor Product

Here, we will define the tensor product of modules. We start with bilinear maps.

Definition 2.18: Let M, N, P be R -modules and $\mathbf{b} : M \times N \rightarrow P$ be a map. $\mathbf{b}$ is called an R -bilinear map if it is linear in each component, explicitly if for any $m, m' \in M$, $n, n' \in N$ and $r \in R$ the following are satisfied;

$$\mathbf{b}(m + m', n) = \mathbf{b}(m, n) + \mathbf{b}(m', n) \text{ and } \mathbf{b}(rm, n) = r\mathbf{b}(m, n) \quad (2.38)$$

$$\mathbf{b}(m, n + n') = \mathbf{b}(m, n) + \mathbf{b}(m, n') \text{ and } \mathbf{b}(m, rn) = r\mathbf{b}(m, n) \quad (2.39)$$

Example 2.16: We give some examples of bilinear map below.

- i) Let R be a ring. Then the map $R \times R \rightarrow R$, $(r, s) \mapsto rs$ is bilinear.
- ii) Determinant function $M_2(R) \rightarrow R$ is bilinear if we identify $M_2(R)$ with $C \times C$ where C is the set module of column vectors with 2-entries over R .

iii) Let M, N, P and Q be R -modules. Let $M \times N \xrightarrow{f} P$ be bilinear and $P \xrightarrow{g} Q$ be linear. Then $M \times N \xrightarrow{g \circ f} Q$ is bilinear.

iv) Let M be an R -module. The map $M \times M \rightarrow M, (x, y) \mapsto x + y$ is not bilinear in general.

Theorem 2.15: Let M, N be R -modules. Then there exists a unique R -module T with a unique R -bilinear map $g : M \times N \rightarrow T$ which satisfies the following property:

Given any R -module P and any R -bilinear map $f : M \times N \rightarrow P$, there exists a unique R -linear map $f' : T \rightarrow P$ such that the following diagram is commutative (i.e. $f' \circ g = f$).

$$\begin{array}{ccc} M \times N & \xrightarrow{g} & T \\ \downarrow f & \swarrow f' & \\ P & & \end{array} \quad (2.40)$$

Proof [Atiyah, 1994] [p: 24] ■

Definition 2.19: Within the notation of the Theorem 2.15, the R -module T is called the tensor product of M and N . We write $T = M \otimes_R N$ or just $M \otimes N$ whenever the ring R is understood.

The Theorem 2.15 is also called the universal property of tensor products. Also we write $g(m, n) = m \otimes n$ where g is the bilinear map described in the Theorem 2.15.

Example 2.17: Let M, N be R -modules, m in M , n in N and $T = M \otimes_R N$. By bilinearity of g we see that $0_M \otimes_R n = (0_M + 0_M) \otimes_R n = 0_M \otimes_R n + 0_M \otimes_R n$. Then $0_T = 0_M \otimes_R n$. Similarly we can obtain $0_T = m \otimes_R 0_N$.

Example 2.18: Let A be a finite abelian group. Then there exists a natural number n such that $n \cdot a = 0_A$ for all $a \in A$. Let $T = \mathbb{Q} \otimes_{\mathbb{Z}} A$. But then for any $a \in A$ and $r \in \mathbb{Q}$, we have that

$$r \otimes a = n \frac{r}{n} \otimes a = \frac{r}{n} \otimes n \cdot a = \frac{r}{n} \otimes 0_A = 0_T \quad (2.41)$$

by bilinearity. Then $\mathbb{Q} \otimes_{\mathbb{Z}} A = 0$.

Example 2.19: Let a, b be integers such that $\gcd(a, b) = 1$. Then there exist integers x_a and x_b such that $x_a a + x_b b = 1$. But then for any $\bar{m} \in \mathbb{Z}/a\mathbb{Z}$ and $\bar{n} \in \mathbb{Z}/b\mathbb{Z}$ we have

$$\begin{aligned}
\bar{m} \otimes \bar{n} &= (x_a a + x_b b) \cdot (m \otimes n) \\
&= x_a a \cdot (m \otimes n) + x_b b \cdot (m \otimes n) \\
&= x_a \cdot (a \cdot m \otimes n) + x_b \cdot (m \otimes b \cdot n) \\
&= x_a \cdot (\bar{0} \otimes n) + x_b \cdot (m \otimes \bar{0}) = 0
\end{aligned} \tag{2.42}$$

So we see that $\mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} = 0$.

2.2.3. Tensor Products of Algebras Over a Field

Any R -algebra is an R -module by definition. A module over a field is a vector space, so in particular any algebra over a field is a vector space.

Theorem 2.16: Let $\mathbb{k}$ be field and $\mathcal{A}, \mathcal{B}$ be $\mathbb{k}$ -algebras. Then $\mathcal{A} \otimes_{\mathbb{k}} \mathcal{B}$ is a $\mathbb{k}$ -algebra under the following operation

$$(a \otimes_{\mathbb{k}} b) \cdot (a' \otimes_{\mathbb{k}} b') = (aa' \otimes_{\mathbb{k}} bb') \tag{2.43}$$

for any $a, a' \in \mathcal{A}$ and $b, b' \in \mathcal{B}$.

Proof [Brešar, 2014] [p: 87-88] ■

Definition 2.20: Let $\mathcal{A}$ be a central simple $\mathbb{k}$ -algebra. We define the opposite algebra of $\mathcal{A}$ denoted by $\mathcal{A}^o$ as the $\mathbb{k}$ -algebra whose underlying set and addition law is the same as $\mathcal{A}$ but multiplication is given by $a * b = b \cdot a$ for $a, b \in \mathcal{A}$.

We say that a k -algebra $\mathcal{A}$ is finite-dimensional if $\mathcal{A}$ is a finite-dimensional k -vector space.

Theorem 2.17: (Wedderburn-Artin) Let $\mathcal{A}$ be a finite-dimensional simple $\mathbb{k}$ -algebra. Then there exists a positive integer n and a division algebra D such that $\mathcal{A} \cong \mathcal{M}_n(D)$

where D is unique up to isomorphism.

Proof [Brešar, 2014] [p: 42-44] ■

A particular but extremely important consequence of the Wedderburn-Artin theorem is about the classification of central simple algebras.

Corollary 2.4: Let $\mathcal{A}$ be a finite-dimensional central simple $\mathbb{k}$ -algebra. Then there exists a positive integer n and a central division algebra D such that $\mathcal{A} \cong \mathcal{M}_n(D)$ where D is unique up to isomorphism.

Proof [Brešar, 2014] [p: 44] ■

We will use the Corollary 2.4 to define equivalence classes of central simple algebras. First, we need to give some basic properties of the tensor product of algebras.

Lemma 2.2: Let $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ be $\mathbb{k}$ -algebras and m, n be positive integers. Then,

- i) $\mathcal{A} \otimes_{\mathbb{k}} \mathcal{B} \cong \mathcal{B} \otimes_{\mathbb{k}} \mathcal{A}$
- ii) $(\mathcal{A} \otimes_{\mathbb{k}} \mathcal{B}) \otimes_{\mathbb{k}} \mathcal{C} \cong \mathcal{A} \otimes_{\mathbb{k}} (\mathcal{B} \otimes_{\mathbb{k}} \mathcal{C})$
- iii) $\mathcal{A} \otimes_{\mathbb{k}} \mathbb{k} \cong \mathcal{A}$ and $\mathbb{k} \otimes_{\mathbb{k}} \mathcal{B} \cong \mathcal{B}$
- iv) $\mathcal{M}_n(\mathbb{k}) \otimes_{\mathbb{k}} \mathcal{A} \cong \mathcal{M}_n(\mathcal{A})$
- v) $\mathcal{M}_n(\mathbb{k}) \otimes_{\mathbb{k}} \mathcal{M}_m(\mathbb{k}) \cong \mathcal{M}_{mn}(\mathbb{k})$
- vi) $\mathcal{A} \otimes_{\mathbb{k}} \mathcal{A}^o \cong \mathcal{M}_n(\mathbb{k})$ where $n = [\mathcal{A} : \mathbb{k}]$

Proof See p: 26 of [Atiyah, 1994] for i) - iii) and p: 87-92 of [Brešar, 2014] for iv) - vi) Note that i) - iii) actually hold if we replace $\mathbb{k}$ and the given algebras by any ring R and R -modules respectively. ■

We will also need a general version of associativity of the tensor product.

Lemma 2.3: Let R and S be rings. Let M be an R -module, N and L be (R, S) -bimodules. Then there is a unique isomorphism of abelian groups

$$(M \otimes_R N) \otimes_S L \cong M \otimes_R (N \otimes_S L) \quad (2.44)$$

Moreover, if M is additionally a T -module for some ring T , then this isomorphism is T -linear, and so is an isomorphism of T -modules.

Proof [Dummit and Foote, 2004][p: 371] ■

Theorem 2.18: Let $\mathbb{k}$ be a field and D, D' be division $\mathbb{k}$ algebras. If $\mathcal{M}_m(D) \cong \mathcal{M}_n(D')$ for some positive integers m and n then $m = n$ and $D \cong D'$.

Proof [Chen, 2019] [p: 5-6] ■

Theorem 2.19: Let $\mathbb{k}$ be a field and $\mathcal{A}, \mathcal{B}$ be central simple $\mathbb{k}$ -algebras. Then $\mathcal{A} \otimes_{\mathbb{k}} \mathcal{B}$ is a central simple $\mathbb{k}$ -algebra.

Proof [Lerner, 2007] [p: 25] ■

Theorem 2.20: Let $\mathcal{A} \cong \mathcal{M}_m(D)$ and $\mathcal{B} \cong \mathcal{M}_n(D')$ be finite-dimensional central simple $\mathbb{k}$ -algebras where D and D' are division rings. The following conditions are equivalent.

- i) $D \cong D'$.
- ii) There exist positive integers m and n such that $\mathcal{A} \otimes_{\mathbb{k}} \mathcal{M}_n(\mathbb{k}) \cong \mathcal{B} \otimes_{\mathbb{k}} \mathcal{M}_m(\mathbb{k})$.
- iii) There exist positive integers m and n such that $\mathcal{M}_n(\mathcal{A}) \cong \mathcal{M}_m(\mathcal{B})$.

Proof

$i \implies ii$: Let $D \cong D'$. Then

$$\mathcal{A} \otimes \mathcal{M}_n(\mathbb{k}) \cong \mathcal{M}_n(\mathcal{A}) \cong \mathcal{M}_n(\mathcal{M}_m(D)) \cong \mathcal{M}_{mn}(D) \tag{2.45}$$

$$\mathcal{B} \otimes \mathcal{M}_m(\mathbb{k}) \cong \mathcal{M}_m(\mathcal{B}) \cong \mathcal{M}_m(\mathcal{M}_n(D')) \cong \mathcal{M}_{mn}(D')$$

Then $\mathcal{A} \otimes \mathcal{M}_n(\mathbb{k}) \cong \mathcal{B} \otimes \mathcal{M}_m(\mathbb{k})$ since $D \cong D'$.

$ii \implies iii$: Direct result of Lemma 2.2. iv)

$iii \implies i$: Let $\mathcal{M}_n(\mathcal{A}) \cong \mathcal{M}_m(\mathcal{B})$. Then

$$\Rightarrow \mathcal{M}_n(\mathcal{M}_m(D)) \cong \mathcal{M}_m(\mathcal{M}_n(D'))$$

$$\Rightarrow \mathcal{M}_{nm}(D) \cong \mathcal{M}_{mn}(D') \quad (2.46)$$

$$\Rightarrow D \cong D' \text{ by the Theorem 2.18}$$

■

Definition 2.21: Let $\mathcal{A} \cong \mathcal{M}_m(D)$ and $\mathcal{B} \cong \mathcal{M}_n(D')$ be finite-dimensional central simple $\mathbb{k}$ -algebras where D and D' are division rings. We say that $\mathcal{A}$ and $\mathcal{B}$ are similar and we write $\mathcal{A} \sim \mathcal{B}$ if one of the conditions of the Theorem 2.20 is satisfied.

Note that " $\sim$ " is an equivalence relation by Lemma 2.2. We will use this definition to construct Brauer groups in the next section.

2.2.4. Quaternion Algebras

In this section, we introduce an important class of algebras for this work. We take $\mathbb{k}$ to be a field of characteristic not equal to 2 in this section.

Definition 2.22: Let α, β be non-zero elements of $\mathbb{k}$. The quaternion algebra depending on α and β denoted by $\left(\frac{\alpha, \beta}{\mathbb{k}}\right)$ is defined as

$$\left(\frac{\alpha, \beta}{\mathbb{k}}\right) = \frac{\mathbb{k} \langle i, j, k \rangle}{\langle i^2 - \alpha, j^2 - \beta, ij + ji, ij - k \rangle} \quad (2.47)$$

Note that $\left(\frac{\alpha, \beta}{\mathbb{k}}\right)$ is a 4-dimensional algebra over $\mathbb{k}$ with a basis $\{1, i, j, k\}$.

Example 2.20: Hamilton's quaternions $\mathbb{H} = \left(\frac{-1, -1}{\mathbb{R}}\right)$.

Example 2.21: $M_2(\mathbb{k}) \cong \left(\frac{1, 1}{\mathbb{k}}\right)$.

Proof Let

$$I = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (2.48)$$

so that $\{I, J, K, I_2\}$ is a basis for $M_2(\mathbb{k})$. Let $\phi : M_2(\mathbb{k}) \rightarrow \left(\frac{1, 1}{\mathbb{k}}\right)$ be defined as

$$\phi(I) = i, \phi(J) = j, \phi(K) = k, \phi(I_2) = 1 \quad (2.49)$$

and extended to whole $M_2(\mathbb{k})$ k -linearly. By the identities $I^2 = J^2 = I_2$, $IJ = K$ and $IJ + JI = 0$ we see that ϕ is a k -algebra homomorphism. But ϕ is bijective and so is a k -algebra isomorphism. ■

Theorem 2.21: Let α, β be non-zero elements of $\mathbb{k}$ and $H = \left(\frac{\alpha, \beta}{\mathbb{k}}\right)$. Then

- i) H is a central simple $\mathbb{k}$ -algebra.
- ii) Either H is a division algebra or is isomorphic to $M_2(\mathbb{k})$.
- iii) H is a division algebra if and only if $(\alpha, \beta)_{\mathbb{k}} = -1$.

Proof The reader is referred to [Voight, 2020][p: 94] and to [Robert, 2009][p: 36]. ■

If we take $\mathbb{k} = \mathbb{Q}_p$ in the part iii) of Theorem 2.21, we reach the following result.

Corollary 2.5: $\left(\frac{\alpha, \beta}{\mathbb{Q}_p}\right) \cong M_2(\mathbb{Q}_p)$ if and only if $(\alpha, \beta)_p = 1$.

2.2.5. Extension of Scalars

Let $\mathbb{K}/\mathbb{k}$ be a field extension, so in particular $\mathbb{K}$ is a $\mathbb{k}$ -vector space. By using tensor products we can extend any $\mathbb{k}$ -algebra to a $\mathbb{K}$ -algebra with the following theorem.

Theorem 2.22: (Extension of Scalars) Let $\mathcal{A}$ be a $\mathbb{k}$ -algebra and $\mathbb{K}/\mathbb{k}$ be a field extension. Then $\mathbb{K} \otimes_{\mathbb{k}} \mathcal{A}$ is a $\mathbb{K}$ -algebra with the following multiplication:

$$\alpha(\mu \otimes_{\mathbb{k}} a) = (\alpha\mu) \otimes_{\mathbb{k}} a \quad \text{for all } \alpha, \mu \in \mathbb{K}, a \in \mathcal{A} \quad (2.50)$$

We call $\mathbb{K} \otimes_{\mathbb{k}} \mathcal{A}$ the extension of scalars of $\mathcal{A}$ by $\mathbb{K}$ and denote it by $\mathcal{A}_{\mathbb{K}} = \mathbb{K} \otimes_{\mathbb{k}} \mathcal{A}$.

Proof [Brešar, 2014][p: 94] ■

Definition 2.23: Let $\mathcal{A}$ be a finite-dimensional central simple $\mathbb{k}$ -algebra and $\mathbb{K}/\mathbb{k}$ be a field extension. $\mathbb{K}$ is called a splitting field for $\mathcal{A}$ if $\mathcal{A}_{\mathbb{K}} \cong \mathcal{M}_n(\mathbb{K})$. In this case we also say that $\mathbb{K}$ splits $\mathcal{A}$, $\mathcal{A}$ is split over $\mathbb{K}$ or just $\mathcal{A}_{\mathbb{K}}$ is split.

Example 2.22: Let $\mathbb{H} = \left(\frac{-1, -1}{\mathbb{R}} \right)$ (the Hamilton's quaternions). Since $(-1, -1)_{\mathbb{R}} = -1$, by Theorem 2.21 we see that $\mathbb{H}$ is not isomorphic to $M_2(\mathbb{R})$.

Now if $\mathbb{k}$ is an algebraically closed field, then $(\alpha, \beta)_{\mathbb{k}} = 1$ for any nonzero $\alpha, \beta \in \mathbb{k}$. This is simply because of the fact that any element has a square root in $\mathbb{k}$. So that if H is a quaternion algebra over $\mathbb{k}$ then H is split by Theorem 2.21. In particular $\mathbb{H}$ is split over $\mathbb{C}$, but not split over $\mathbb{R}$.

3. THE BRAUER GROUP

This section is devoted to the definition and basic properties of Brauer groups which is the core object for this work. The algebraic tools required to define Brauer groups are already given in the previous Chapter. We will mainly use the Definition 2.21 and the Lemma 2.2.

3.1. Brauer Group of a Field

Theorem 3.1: (Brauer Group of Fields) Let $\mathbb{k}$ be a field. Then, the set of all equivalence classes of finite-dimensional central simple $\mathbb{k}$ -algebras is an abelian group where the group operation is defined by $[\mathcal{A}] \cdot [\mathcal{B}] = [\mathcal{A} \otimes_{\mathbb{k}} \mathcal{B}]$ for any central simple $\mathbb{k}$ -algebras $\mathcal{A}$ and $\mathcal{B}$. This group is called the Brauer Group of $\mathbb{k}$ and is denoted by $Br(\mathbb{k})$.

Proof [Chen, 2019][p: 12] Tensor product of two central simple algebras is again central simple algebra by the Theorem 2.19. Then, $Br(\mathbb{k})$ is closed under the above operation. Let $\mathcal{A} \sim \mathcal{A}'$ and $\mathcal{B} \sim \mathcal{B}'$. Then, $\mathcal{M}_n(\mathbb{k}) \otimes_{\mathbb{k}} \mathcal{A} \cong \mathcal{M}_{n'}(\mathbb{k}) \otimes_{\mathbb{k}} \mathcal{A}'$ and $\mathcal{M}_m(\mathbb{k}) \otimes_{\mathbb{k}} \mathcal{B} \cong \mathcal{M}_{m'}(\mathbb{k}) \otimes_{\mathbb{k}} \mathcal{B}'$ for some positive integers m, m', n, n' . Then

$$(\mathcal{M}_n(\mathbb{k}) \otimes_{\mathbb{k}} \mathcal{A}) \otimes_{\mathbb{k}} (\mathcal{M}_m(\mathbb{k}) \otimes_{\mathbb{k}} \mathcal{B}) \cong \mathcal{M}_{mn}(\mathbb{k}) \otimes_{\mathbb{k}} (\mathcal{A} \otimes_{\mathbb{k}} \mathcal{B}) \quad (3.1)$$

$$(\mathcal{M}_{n'}(\mathbb{k}) \otimes_{\mathbb{k}} \mathcal{A}') \otimes_{\mathbb{k}} (\mathcal{M}_{m'}(\mathbb{k}) \otimes_{\mathbb{k}} \mathcal{B}') \cong \mathcal{M}_{m'n'}(\mathbb{k}) \otimes_{\mathbb{k}} (\mathcal{A}' \otimes_{\mathbb{k}} \mathcal{B}') \quad (3.2)$$

Hence, $\mathcal{M}_{mn}(\mathbb{k}) \otimes_{\mathbb{k}} (\mathcal{A} \otimes_{\mathbb{k}} \mathcal{B}) \cong \mathcal{M}_{m'n'}(\mathbb{k}) \otimes_{\mathbb{k}} (\mathcal{A}' \otimes_{\mathbb{k}} \mathcal{B}')$. This means that $\mathcal{A} \otimes_{\mathbb{k}} \mathcal{B} \sim \mathcal{A}' \otimes_{\mathbb{k}} \mathcal{B}'$. Therefore, this multiplication is well defined.

Also, the multiplication defined above is associative and commutative. This follows by associativity and commutativity of tensor products. $[\mathbb{k}]$ is the identity element by Lemma 2.2. Finally, the equivalence class of the opposite algebra serves as the inverse. Hence, $Br(\mathbb{k})$ is an abelian group. $\blacksquare$

After defining the Brauer group, we will now need to define the relative Brauer group.

Theorem 3.2: (Relative Brauer Group) Let $\phi : \mathbb{k} \longrightarrow \mathbb{K}$ be a nonzero field homomorphism. ϕ extends to a map $Br(\phi) : Br(\mathbb{k}) \rightarrow Br(\mathbb{K})$ defined as

$$Br(\phi) : Br(\mathbb{k}) \longrightarrow Br(\mathbb{K}) \quad (3.3)$$

$$[\mathcal{A}] \longrightarrow [\mathcal{A}_{\mathbb{K}}]$$

where we endow the $\mathbb{k}$ -algebra structure on $\mathbb{K}$ via the map ϕ . $Br(\mathbb{K}/\mathbb{k}) = \text{Ker}(Br(\phi))$ is called the relative Brauer group of $\mathbb{K}/\mathbb{k}$.

Proof [Lerner, 2007] [p: 28-29] ■

In general, we will take $\mathbb{K}/\mathbb{k}$ to be a finite extension and ϕ will be the inclusion map. The elements of the relative Brauer group are finite-dimensional central simple $\mathbb{k}$ -algebras which split over $\mathbb{K}$.

3.2. Double Centralizer Theorem

In general, the center of any algebraic structure is the set of elements that commute with all elements. We will study the centralizer of subsets of an algebra.

Definition 3.1: (Centralizer) Let S be a subset of an algebra $\mathcal{A}$. The centralizer of S in $\mathcal{A}$ is defined as follows:

$$C_{\mathcal{A}}(S) := \{a \in \mathcal{A} | a.s = s.a \text{ for all } s \in S\} \quad (3.4)$$

Lemma 3.1: Let $\mathcal{A}$ be a $\mathbb{k}$ -algebra and S be a subalgebra of $\mathcal{A}$. Then

$$C_{\mathcal{A}}(S) \cong \text{End}_{\mathcal{A} \otimes_{\mathbb{k}} S^{\circ}}(\mathcal{A}) \quad (3.5)$$

Proof Let $a, x \in \mathcal{A}$ and $s \in S$. $\mathcal{A}$ is a right $\mathcal{A} \otimes_{\mathbb{k}} S^{\circ}$ -module with multiplication $x(a \otimes_{\mathbb{k}} s) = sxa$. It is clear that this multiplication is well defined. Also, it is associative by associativity of tensor product. Now, we define a map f as follows:

$$f : C_{\mathcal{A}}(S) \rightarrow \text{End}_{\mathcal{A} \otimes_{\mathbb{k}} S^{\circ}}(\mathcal{A}) \quad (3.6)$$

$$c \mapsto (f_c(s) = cs)$$

This map is well defined since S is a subalgebra of $\mathcal{A}$. Let $c \in C_{\mathcal{A}}(S)$ and $a \otimes_{\mathbb{k}} s \in \mathcal{A} \otimes_{\mathbb{k}} S^{\circ}$. Then,

$$f_c(x(a \otimes_{\mathbb{k}} s)) = f_c(sxa) = csxa \quad (3.7)$$

Also

$$f_c(x).(a \otimes_{\mathbb{k}} s)) = cx(a \otimes_{\mathbb{k}} s) = scxa = csxa \quad (3.8)$$

Then, f is a $\mathcal{A} \otimes_{\mathbb{k}} S^\circ$ -endomorphism. Hence, f is well defined. Let $c, c' \in C_{\mathcal{A}}(S)$ and $x \in \mathcal{A}$. Then,

$$f_{cc'}(a) = cc'x = c(f_{c'}(a)) = f_c(f_{c'}(a)) = f_c \circ f_{c'}(a) \quad (3.9)$$

Therefore f is a module homomorphism. Now we show that f is one-to-one and onto.

Let m be an element of $\text{Ker}(f)$, then $f_m(x) = mx = 0$ for any $x \in \mathcal{A}$. If we take $x = 1$, then $f_m(1) = m1 = m = 0$. Therefore, $\text{Ker}(f) = \{0\}$ and f is one to one. Now, we show that f is onto. Let $\alpha \in \text{End}_{\mathcal{A} \otimes_{\mathbb{k}} S^\circ}(\mathcal{A})$ and $c = \alpha(1)$. For all $s \in S$ we have

$$sc = c(1 \otimes_{\mathbb{k}} s) = \alpha(1)(1 \otimes_{\mathbb{k}} s) = \alpha(1(1 \otimes_{\mathbb{k}} s)) = \alpha(s) \quad (3.10)$$

Also,

$$cs = c(s \otimes_{\mathbb{k}} 1) = \alpha(1)(s \otimes_{\mathbb{k}} 1) = \alpha(1(s \otimes_{\mathbb{k}} 1)) = \alpha(s). \quad (3.11)$$

Then, c is commutative for all elements of S . Then $c \in C_{\mathcal{A}}(S)$. Therefore f is onto. ■

Theorem 3.3: (Double Centralizer Theorem) Let $\mathcal{A} \cong \mathcal{M}_m(D)$ be a finite-dimensional central simple $\mathbb{k}$ -algebra where D is a division algebra and S is a simple subalgebra of $\mathcal{A}$. Then,

i) $C_{\mathcal{A}}(S)$ is simple.

ii) If $S \otimes_{\mathbb{k}} D^\circ \cong \mathcal{M}_m(E)$, then $C_{\mathcal{A}}(S) \cong \mathcal{M}_t(E^\circ)$.

iii) $[\mathcal{A} : \mathbb{k}] = [S : \mathbb{k}].[C_{\mathcal{A}}(S) : \mathbb{k}]$.

iv) $C_{\mathcal{A}}(C_{\mathcal{A}}(S)) = S$.

Proof [Farb and Dennis, 2012][p: 94-95] ■

Definition 3.2: (Maximal Subfield) Let $\mathcal{A}$ be a simple algebra over $\mathbb{k}$. A subfield $\mathbb{K}$ of $\mathcal{A}$ is called a maximal subfield if $C_{\mathcal{A}}(\mathbb{K}) = \mathbb{K}$.

Lemma 3.2: Let $\mathbb{k}$ be an algebraically closed field. Then the only finite-dimensional division algebra over $\mathbb{k}$ is itself.

Proof [Chen, 2019][p: 13] ■

Example 3.1: Let D be a finite-dimensional division algebra over $\mathbb{C}$. Then $D \cong \mathbb{C}$.

Corollary 3.1: Let $\mathbb{k}$ be an algebraically closed field and $\mathcal{A}$ be a $\mathbb{k}$ -algebra, then $\mathcal{A}$ is split.

Proof $\mathcal{A} \cong \mathcal{M}_n(D)$ for some division ring. Also D is finite-dimensional $\mathbb{k}$ -algebra. But $\mathbb{k}$ is algebraically closed. Therefore $D = \mathbb{k}$ and $\mathcal{A} \cong \mathcal{M}_n(\mathbb{k})$. Therefore $\mathcal{A}$ is split. ■

By the Corollary 3.1, if $\mathcal{A}$ is a $\mathbb{k}$ -algebra then $\mathcal{A} \otimes_{\mathbb{k}} \mathbb{k}^c \cong \mathcal{M}_n(\mathbb{k}^c)$ where $\mathbb{k}^c$ is the algebraic closure of $\mathbb{k}$.

Corollary 3.2: Let $\mathcal{A}$ be a central simple algebra over $\mathbb{k}$. Then $[\mathcal{A} : \mathbb{k}]$ is a square.

Proof Let $\mathbb{k}^c$ be algebraic closure of $\mathbb{k}$. Then,

$$[\mathcal{A} : \mathbb{k}] = [\mathcal{A} \otimes_{\mathbb{k}} \mathbb{k}^c : \mathbb{k} \otimes_{\mathbb{k}} \mathbb{k}^c] = [\mathcal{A} \otimes_{\mathbb{k}} \mathbb{k}^c : \mathbb{k}^c] = [\mathcal{M}_n(\mathbb{k}^c) : \mathbb{k}^c] = n^2 \quad (3.12)$$
■

Theorem 3.4: Let $\mathcal{A}$ be a central simple $\mathbb{k}$ -algebra and S be a subfield of $\mathcal{A}$ such that S contains $\mathbb{k}$. Then the following are equivalent;

i) $S = C_{\mathcal{A}}(S)$

ii) $[\mathcal{A} : \mathbb{k}] = [S : \mathbb{k}]^2$

iii) S is a maximal commutative $\mathbb{k}$ – subalgebra of $\mathcal{A}$

Proof [Web 7, 2020] [p: 133] ■

One of our aims is to express $Br(\mathbb{k})$ in terms of $Br(\mathbb{K}/\mathbb{k})$ for some extensions $\mathbb{K}/\mathbb{k}$ to be specified later. Recall that $Br(\mathbb{K}/\mathbb{k})$ consists of equivalence classes of central simple $\mathbb{k}$ -algebras which split over $\mathbb{K}$. But up to now we only know splitting of such algebras over an algebraic closure which is not satisfactory. First, we see splitting of division rings.

Theorem 3.5: Let D be a central division $\mathbb{k}$ -algebra. Suppose that $[D : \mathbb{k}] = m^2$ for some positive integer m . If $\mathbb{K}$ is any maximal subfield of D then D splits over $\mathbb{K}$ and $[\mathbb{K} : \mathbb{k}] = m$.

Proof [Farb and Dennis, 2012] [p: 96] ■

So we see that existence of a maximal subfield of a division algebra is a must for the splitting, but the above theorem does not guarantee it. The next theorem will overcome this existence problem.

Theorem 3.6: (Jacobson- Noether Theorem) Let D be a division ring, $\mathbb{k}$ be a field. Suppose that D is a $\mathbb{k}$ -algebra. Then there exists a maximal subfield of D which is a separable extension of $\mathbb{k}$.

Proof [Lerner, 2007] [p: 31] ■

Jacobson- Noether Theorem guarantees the existence of splitting fields of division algebras. But it actually says more than this as we see below.

Corollary 3.3: If D is a central division $\mathbb{k}$ -algebra of degree n^2 over $\mathbb{k}$, then there exists a finite Galois extension $\mathbb{K}/\mathbb{k}$ where $\mathbb{K}$ is a splitting field for D .

Proof [Farb and Dennis, 2012][p: 116] We know that D has a maximal subfield $\mathbb{L}$ which is separable over $\mathbb{k}$ by the Theorem 3.6. Also by Theorem 3.5, we know that $D \otimes_{\mathbb{k}} \mathbb{L} = M_n(\mathbb{L})$.

Let $\mathbb{K}$ be the normal closure of $\mathbb{L}$. Then $\mathbb{K}$ is a Galois extension of $\mathbb{k}$ as it is both a normal and separable extension of $\mathbb{k}$. Also the extension $\mathbb{K}/\mathbb{k}$ is finite since D is finite-dimensional. Therefore $\mathbb{K}/\mathbb{k}$ is a finite Galois extension. Now we need to show that $\mathbb{K}$ splits D .

$$D \otimes_{\mathbb{k}} \mathbb{K} \cong D \otimes_{\mathbb{k}} (L \otimes_L \mathbb{K}) \quad (\text{by part iii) of Lemma 2.2})$$

$$\cong (D \otimes_{\mathbb{k}} L) \otimes_L \mathbb{K} \quad (\text{by Lemma 2.3})$$

(3.13)

$$\cong \mathcal{M}_n(L) \otimes_L \mathbb{K} \quad (\text{since } L \text{ splits } D)$$

$$\cong \mathcal{M}_n(\mathbb{K}) \quad (\text{by part iv) of Lemma 2.2})$$

Therefore $\mathbb{K}$ is a splitting field for D . ■

Now we may state an important theorem for the splitting of central simple algebras which is a core fact for the Brauer groups.

Theorem 3.7: Let $\mathbb{k}$ be a field.

- i) *Let $\mathcal{A}$ be a central simple $\mathbb{k}$ -algebra whose dimension over $\mathbb{k}$ is n^2 and $\mathbb{K}$ be a maximal subfield of $\mathcal{A}$. Then $\mathbb{K}$ is a splitting field for $\mathcal{A}$ and $[\mathcal{A} : \mathbb{K}] = [\mathbb{K} : \mathbb{k}] = n$*
- ii) *Let $\mathbb{K}$ be a field extension of $\mathbb{k}$ with degree n . Then in any equivalence class in $Br(\mathbb{K}/\mathbb{k})$ there exists a unique central simple $\mathbb{k}$ -algebra $\mathcal{A}$ which contains $\mathbb{K}$ as a maximal subfield and has degree n^2 over $\mathbb{k}$.*

Proof [Farb and Dennis, 2012] [p: 115] ■

Note that Theorem 3.5 and part i) of Theorem 3.7 are reminiscent but not identical. In both of these theorems, we see that existence of a maximal subfield of the concerned algebra is a must for the splitting.

Let D be a central division algebra over $\mathbb{k}$. Take $\mathcal{A} = M_n(D)$ which contains $\mathbb{K}$ as a maximal subfield. The above theorem says if $[\mathcal{A} : \mathbb{k}]$ is square then $\mathcal{A}$ is $\mathbb{K}$ split, i.e. $\mathcal{A} \otimes_{\mathbb{k}} \mathbb{K} = M_n(\mathbb{K})$. Also we know $[\mathcal{A}] = [D]$ in $Br(\mathbb{k})$. Then $[\mathcal{A} \otimes_{\mathbb{k}} \mathbb{K}] = [D \otimes_{\mathbb{k}} \mathbb{K}]$. So $\mathbb{K}$ is a splitting field for D i.e. $D \otimes_{\mathbb{k}} \mathbb{K} = M_n(\mathbb{K})$.

Theorem 3.8: $Br(\mathbb{k}) \cong \bigcup Br(\mathbb{K}/\mathbb{k})$, where $\mathbb{K}$ runs over the finite Galois extensions of $\mathbb{k}$.

Proof Let $\mathcal{A} \cong \mathcal{M}_n(D)$ be a $\mathbb{k}$ -algebra and D be a division ring for which $\mathbb{K}$ is a maximal subfield of D . By the Corollary 3.3 $\mathbb{K}$ splits D . Also we know $[\mathcal{A}] = [D]$.

Then we have one to one and onto correspondence between Galois extensions of $\mathbb{k}$ and central simple $\mathbb{k}$ -algebras. Now we define a map to show isomorphism. Let

$$\pi : Br(\mathbb{k}) \longrightarrow \bigcup Br(\mathbb{K}/\mathbb{k}) \quad (3.14)$$

$$[D] \longrightarrow [D_{\mathbb{K}}]$$

We know that this map is well defined, one to one and onto. We will show that this map is a group homomorphism.

Let D, D' be a division ring. Then,

$$\begin{aligned} \pi(D) \cdot \pi(D') &= [D \otimes_{\mathbb{k}} \mathbb{K}] \cdot [D' \otimes_{\mathbb{k}} \mathbb{K}] \\ &= [(D \otimes_{\mathbb{k}} \mathbb{K}) \otimes_{\mathbb{k}} (D' \otimes_{\mathbb{k}} \mathbb{K})] \\ &= [D \otimes_{\mathbb{k}} (\mathbb{K} \otimes_{\mathbb{k}} D') \otimes_{\mathbb{k}} \mathbb{K}] \\ &= [D \otimes_{\mathbb{k}} (D' \otimes_{\mathbb{k}} \mathbb{K}) \otimes_{\mathbb{k}} \mathbb{K}] \\ &= [(D \otimes_{\mathbb{k}} D') \otimes_{\mathbb{k}} \mathbb{K}] \\ &= \pi(D \otimes_{\mathbb{k}} D') \end{aligned} \quad (3.15)$$

■

Now, we examine some basic examples of the Brauer group.

Example 3.2: $Br(\mathbb{k}^c) \cong 1$

It can be seen directly as a result of Lemma 3.2.

Example 3.3: $Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$

We know any finite-dimensional division algebra of $\mathbb{R}$ is isomorphic to one of the $\mathbb{R}, \mathbb{H}$ or $\mathbb{C}$ by Frobenius theorem. But $\mathbb{C}$ is not simple. Then $\mathbb{R}$ has two non-isomorphic finite-dimensional division algebras. Therefore $Br(\mathbb{R})$ has only two elements.

Example 3.4: $Br(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$. We will see this example in details in the last chapter.

3.3. Brauer Group of a Ring

In this part, we will define the Brauer groups of rings. To do that, we need to replace the base field and the central simple algebras over this base field with a ring and Azumaya algebras respectively. So we shall start by defining the Brauer group of a commutative ring.

Definition 3.3: (Enveloping Algebra) Let R be a commutative ring and $\mathcal{A}$ be an R -algebra. The enveloping algebra of $\mathcal{A}$ denoted by $\mathcal{A}^e$ is defined as $\mathcal{A}^e = \mathcal{A} \otimes_R \mathcal{A}^o$

We have a natural homomorphism as follows:

$$\psi_{\mathcal{A}} : \mathcal{A} \otimes_R \mathcal{A}^o \longrightarrow \text{End}_R(\mathcal{A}) \quad (3.16)$$

$$(a \otimes_R a') \longrightarrow \psi_{(a \otimes a')}(x) = axa'$$

Definition 3.4: (Azumaya Algebra) An R -algebra $\mathcal{A}$ is called an Azumaya algebra if the following two conditions hold:

- i) R -module $\mathcal{A}$ is finitely generated, faithful and projective.
- ii) $\mathcal{A}^e \cong \text{End}_R(\mathcal{A})$ (with Homomorphism (3.16))

Example 3.5: Let P be a finitely generated projective R -module. Then the ring $\text{End}_R(P)$ which is seen as an R -algebra is an Azumaya algebra over R [Drensky et al, 1998][p: 253].

Now, we show a relation between Azumaya algebras and central simple algebras.

Proposition 3.1: Let $\mathbb{k}$ be a field and $\mathcal{A}$ be a $\mathbb{k}$ -algebra. Then $\mathcal{A}$ is a central simple algebra if and only if $\mathcal{A}$ is an Azumaya Algebra.

Proof [Farb and Dennis, 2012][p: 186] Let $\mathcal{A}$ be a central simple $\mathbb{k}$ -algebra. Any module over $\mathbb{k}$ is a free module since $\mathbb{k}$ is field. Then $\mathcal{A}$ is finite-dimensional, projective and faithful. Also

$$\mathcal{A}^e := \mathcal{A} \otimes_{\mathbb{k}} \mathcal{A}^o \cong \mathcal{M}_n(\mathbb{k}) \cong \text{End}_{\mathbb{k}}(\mathcal{A}) \quad (3.17)$$

Then $\mathcal{A}$ is an Azumaya algebra.

Let $\mathcal{A}$ be an Azumaya algebra. Then $\mathcal{A}$ is a finite-dimensional over $\mathbb{k}$. Then $\mathcal{A} \cong \mathbb{k}^n$. Then $\mathcal{A}^e \cong \text{End}_{\mathbb{k}}(\mathcal{A}) \cong \text{End}_{\mathbb{k}}(\mathbb{k}^n) \cong \mathcal{M}_n(\mathbb{k})$. Then $\mathcal{A} \otimes_{\mathbb{k}} \mathcal{A}^o$ is a central simple algebra. So $\mathcal{A}$ must be a central simple algebra. ■

Definition 3.5: Let $\mathcal{A}$ and $\mathcal{B}$ be Azumaya algebras over R . We say $\mathcal{A}$ and $\mathcal{B}$ are similar and write $\mathcal{A} \sim \mathcal{B}$ if $\mathcal{A} \otimes_R \text{End}_R(P) \cong \mathcal{B} \otimes_R \text{End}_R(Q)$ for some faithful and projective R -modules P and Q .

Theorem 3.9: The relation " $\sim$ " on Azumaya algebras over R is an equivalence relation.

Proof [Farb and Dennis, 2012] [p: 191] ■

Theorem 3.10: (Brauer Group of Commutative Ring) With the notation of the Theorem 3.9, the set of equivalence classes of Azumaya algebras is a group with the following operation.

$$[\mathcal{A}] \cdot [\mathcal{B}] = [\mathcal{A} \otimes \mathcal{B}] \quad (3.18)$$

This group is called the Brauer group of a commutative ring R and denoted by $\text{Br}(R)$.

Proof [Farb and Dennis, 2012] [p: 192] ■

Theorem 3.11: Let R, S be commutative rings, f be an element of $\text{Hom}(R, S)$. f extends to map $\text{Br}(f) : \text{Br}(R) \longrightarrow \text{Br}(S)$ defined as

$$\text{Br}(f) : \text{Br}(R) \longrightarrow \text{Br}(S) \quad (3.19)$$

$$[A] \longmapsto [A \otimes_R S]$$

Then $\text{Br}(\cdot)$ is a functor from the category of commutative rings and ring homomorphisms to the category of abelian groups and group homomorphisms.

Proof [Farb and Dennis, 2012] [p: 195] ■

In general, determination of the Brauer group of a ring explicitly is a very difficult problem. One may compare the Brauer groups of a ring R and a residue

field $k = R/I$ for some maximal ideal I of it by the reduction map $R \rightarrow k$. This gives a complete characterization of Azumaya algebras over a local ring, i.e. it is possible to describe all Azumaya algebras of R in terms of the central simple algebras over k . But indeed there is not a complete characterization of Azumaya algebras over an arbitrary ring.

But as we will see, the Brauer-Manin obstruction reduces to determining the Brauer groups of fields which finally turns out to be a much simpler problem. So we do not give any further emphasize on Brauer groups of rings. The reader interested in a deeper theory of Azumaya algebras over a general ring are referred to [Auslander and Goldman, 1960] and [DeMeyer and Ingraham, 1971].

Let $\mathbb{k}$ be a field. By a variety over $\mathbb{k}$, we mean the set of common zeros of a family of polynomials in an ideal in $\mathbb{k}[x_1, \dots, x_n]$. Explicitly V is called a variety over $\mathbb{k}$ if there exists an ideal $I = \langle f_1, \dots, f_m \rangle$ of $\mathbb{k}[x_1, \dots, x_n]$ such that

$$V = \{(a_1, a_2, \dots, a_n) : f(a_1, \dots, a_n) = 0 \text{ for all } f \in I\} \quad (3.20)$$

For the purposes of this work, we avoid the deep theory of algebraic varieties and confine ourselves only to this restrictive definition of varieties and also the next definition.

Definition 3.6: (Brauer Group of a Variety) Let $\mathbb{k}$ be a field and V be a variety over $\mathbb{k}$ given by the ideal I in $\mathbb{k}[x_1, \dots, x_n]$. Let $\mathcal{R}$ be the quotient ring defined as $\mathcal{R} = \mathbb{k}[x_1, \dots, x_n]/\sqrt{I}$ where $\sqrt{I}$ is the radical of I . The Brauer group of V denoted by $Br(V)$ is defined as

$$Br(V) := Br(\mathcal{R}) \quad (3.21)$$

4. FACTOR SETS AND COHOMOLOGY

This chapter is devoted to the relation between Brauer groups and a suitable cohomology group. Indeed we will not use the content of this section directly for applications of Brauer-Manin obstruction. The relation between Brauer groups and certain cohomology groups yield a very important fact about the $Br(\mathbb{Q}_p)$ (See Theorem 5.2 below). But as this theory is beyond the scope of this thesis and the aim of this work is to sketch the Brauer-Manin obstruction, the reader may directly skip this part and pass to the next chapter without any loss in a general understanding of the Brauer-Manin obstruction. In the first section, we start with a correspondence between a relative Brauer group and factor sets, and in the second section, we will pass to the relevant cohomology group. We will restrict to basic and standard facts to define the cohomology of a chain complex and give the deep results as theorems with convenient references.

4.1. Factor Sets and Crossed Product Algebras

Recall that in the previous chapter, we saw that if the dimension of a central simple algebra $\mathcal{A}$ over $\mathbb{k}$ is n^2 , then there exists a maximal subfield $\mathbb{K}$ of $\mathcal{A}$ such that $\mathbb{K}/\mathbb{k}$ is a Galois extension of degree n . In the rest of this section we use this fact without any further emphasize. We also set $G = Gal(\mathbb{K}/\mathbb{k})$.

Theorem 4.1: (Skolem-Noether) Let $\mathcal{A}$ be a finite-dimensional central simple $\mathbb{k}$ -algebra and S, T be simple $\mathbb{k}$ -subalgebras of $\mathcal{A}$. Given any $\mathbb{k}$ -algebra isomorphism $\alpha : S \rightarrow T$ which fixes each element of $\mathbb{k}$, there exists $x_\alpha \in \mathcal{A}$ such that for all $s \in S$, $\alpha(s) = x_\alpha s x_\alpha^{-1}$

Proof [Web 7, 2020] [p: 129] ■

In particular if we take $S = T = \mathbb{K}$, then any $\alpha \in G = Gal(\mathbb{K}/\mathbb{k})$ satisfies the hypothesis of Skolem-Noether Theorem. Therefore for every α in G , we can find $x_\alpha \in \mathcal{A}$ such that $\alpha(s) = x_\alpha s x_\alpha^{-1}$ for any $s \in \mathbb{K}$. In this case we say that x_α satisfies Skolem-Noether theorem for α .

Lemma 4.1: Let $\mathbb{K}/\mathbb{k}$ be a finite Galois extension, $G = Gal(\mathbb{K}/\mathbb{k})$, $\mathcal{A}$ be a

finite-dimensional central simple $\mathbb{K}$ -algebra and $\mathbb{K}$ be a maximal subfield of $\mathcal{A}$. Then the following hold:

i) If $x_\sigma, y_\sigma \in \mathcal{A}$ both satisfy Skolem Noether theorem for $\sigma \in G$, then

$$x_\sigma = k_\sigma y_\sigma \quad \text{for some } k_\sigma \in \mathbb{K}^* \quad (4.1)$$

ii) Let $\sigma, \tau \in G$, and x_σ, x_τ and $x_{\sigma\tau}$ satisfy Skolem-Noether theorem for σ, τ and $\sigma\tau$ respectively. Then we have

$$x_\sigma.x_\tau = k_{\sigma,\tau}.x_{\sigma\tau} \quad \text{for some } k_{\sigma,\tau} \in \mathbb{K}^* \quad (4.2)$$

Proof [Farb and Dennis, 2012][p: 118-119]

i) Let $\sigma(a) = x_\sigma a x_\sigma^{-1} = y_\sigma a y_\sigma^{-1}$ for any $\sigma \in G, a \in \mathbb{K}^*$

$$\Rightarrow x_\sigma a x_\sigma^{-1} = \sigma(a) \Rightarrow x_\sigma y_\sigma^{-1} \sigma(a) y_\sigma x_\sigma^{-1} = \sigma(a) \Rightarrow x_\sigma y_\sigma^{-1} \sigma(a) = \sigma(a) x_\sigma y_\sigma^{-1}$$

$$\Rightarrow x_\sigma y_\sigma^{-1} = k_\sigma \in C_{\mathcal{A}}(\mathbb{K})^* = \mathbb{K}^*$$

$$\Rightarrow x_\sigma = k_\sigma y_\sigma \text{ for some } k_\sigma \in \mathbb{K}^*$$

ii) Let $\sigma, \tau \in G$.

$$\Rightarrow x_{\sigma\tau} a x_{\sigma\tau}^{-1} = \sigma(\tau(a)) = \sigma\tau(a) = x_\sigma \tau(a) x_\sigma^{-1} = x_\sigma x_\tau . a . x_\tau^{-1} x_\sigma^{-1}$$

$$\Rightarrow x_\sigma . x_\tau \text{ and } x_{\sigma\tau} \text{ both satisfy the Skolem Noether theorem for } \sigma\tau.$$

$$\Rightarrow \text{Then by the first part there exists } k_{\sigma\tau} \in \mathbb{K}^* \text{ such that } x_\sigma . x_\tau = k_{\sigma,\tau} . x_{\sigma\tau}.$$

■

To simplify the notation in the rest of the paper we write $\{k_{\sigma,\tau}\}$ and $\{x_\sigma\}$ for the sets $\{k_{\sigma,\tau} \in \mathbb{K}^* : \sigma, \tau \in G\}$ and $\{x_\sigma \in \mathcal{A} : \sigma \in G\}$ respectively which satisfy Lemma 4.1.

Proposition 4.1: $\{x_\sigma\}$ is a basis for $\mathcal{A}$ over $\mathbb{K}$.

Proof [Farb and Dennis, 2012][p: 119] We know $|G| = |\mathbb{K} : \mathbb{k}| = |\mathcal{A} : \mathbb{K}|$. So if we can show that $\{x_\sigma\}$ is a linearly independent subset of $\mathcal{A}$, then the proof will be completed.

Let J be a maximal subset of G for which $J \neq G$ and the set of $\{x_\tau | \tau \in J\}$ is linearly independent. Assume $\sigma \notin J$, then we can write x_σ as a linear combination of the elements of $\{x_\tau | \tau \in J\}$ that is:

$$x_\sigma = \sum_{\tau \in J} k_\tau x_\tau \quad \text{for some } k_\tau \in \mathbb{K} \quad (4.3)$$

$$\Rightarrow x_\sigma r = \sum_{\tau \in J} k_\tau x_\tau r \quad \text{for any } r \in \mathbb{K}$$

$$\Rightarrow \sigma(r)x_\sigma = \sum_{\tau \in J} k_\tau \tau(r)x_\tau \quad \text{by the Theorem 4.1.}$$

Also we have $\sigma(r)x_\sigma = \sigma(r) \sum_{\tau \in J} k_\tau x_\tau$ (multiplying Equation (4.3) by $\sigma(r)$). Then

$$\Rightarrow \sigma(r) \sum_{\tau \in J} k_\tau x_\tau = \sum_{\tau \in J} k_\tau \tau(r)x_\tau$$

$$\Rightarrow \sigma(r) \sum_{\tau \in J} k_\tau x_\tau x_\tau^{-1} = \sum_{\tau \in J} k_\tau \tau(r)x_\tau x_\tau^{-1}$$

$$\Rightarrow \sum_{\tau \in J} \sigma(r)k_\tau = \sum_{\tau \in J} k_\tau \tau(r)$$

$\Rightarrow \sigma(r)k_\tau = k_\tau \tau(r)$ for all $\tau \in J, r \in \mathbb{K}$. There exists $\tau \in J$ and $x_\tau \neq 0$ since x_σ can not be equal to zero. we see that $\tau(r) = \sigma(r)$ and hence $J = G$.

■

We can rewrite Proposition 4.1 in a different way.

Corollary 4.1:

We have that

$$\mathcal{A} = \bigoplus_{\sigma \in G} \mathbb{K}.x_\sigma \quad (4.4)$$

Definition 4.1: (Factor Set) Let $\mathcal{A}$ be a central simple $\mathbb{k}$ -algebra and $\mathbb{K}$ be a maximal subfield of $\mathcal{A}$. The collection $\{k_{\sigma, \tau}\}$ given in part ii) of Lemma 4.1 is called a factor set of $\mathcal{A}$ depending on $\mathbb{K}$.

Definition 4.2: The factor set of $\{k_{id, \tau}\}$ for $1_{\mathcal{A}} \in \{x_{id}\}$ is called normalised.

Up to now we associated to a given a central simple $\mathbb{k}$ -algebra $\mathcal{A}$ a special subset, namely a factor set $\{k_{\sigma,\tau}\}$ of $\mathbb{K}$. The next result clarifies when we can associate to any subset $\{k_{\sigma,\tau}\}$ a central simple $\mathbb{k}$ -algebra.

Theorem 4.2: Let $\mathbb{K}/\mathbb{k}$ be a finite Galois extension. A subset $\{k_{\sigma,\tau}\}$ of $\mathbb{K}$ is a factor set of some central simple $\mathbb{k}$ -algebra $\mathcal{A}$ if it satisfies

$$\rho(k_{\sigma,\tau}) \cdot k_{\rho,\sigma\tau} = k_{\rho,\sigma} \cdot k_{\rho\sigma,\tau}, \text{ for all } \sigma, \tau, \rho \in G. \quad (4.5)$$

Moreover in this case $\mathcal{A}$ contains $\mathbb{K}$ as a maximal subfield.

Proof [Farb and Dennis, 2012][p: 120-121] ■

Now we see an interesting fact about factor sets. Condition (4.5) of Theorem 4.2 is actually independent of the central simple $\mathbb{k}$ -algebra $\mathcal{A}$, it is just an equality involving elements of $\mathbb{K}$. So it is reasonable to call any subset $\{k_{\sigma,\tau}\}$ of $\mathbb{K}$ which satisfies condition (4.5) of Theorem 4.2 as a factor set depending on $\mathbb{K}$ regardless of the concerned algebra. So Theorem 4.2 leads to the idea to establish a correspondence between central simple $\mathbb{k}$ -algebras which admit $\mathbb{K}$ as a maximal subfield and factor sets depending on $\mathbb{K}$ in this new sense. But we will achieve this when we consider suitable equivalence classes.

Theorem 4.3: Let $\mathbb{K}/\mathbb{k}$ be a finite Galois extension, $\{a_{\sigma,\tau}\}$ and $\{b_{\sigma,\tau}\}$ be two factor sets corresponding to $\{x_\sigma\}$ and $\{y_\sigma\}$ respectively. Let $k_\sigma, k_\tau, k_{\sigma\tau} \in \mathbb{K}^*$ be the corresponding elements satisfying condition (4.1) and condition (4.2) of Lemma 4.1. We write $\{a_{\sigma,\tau}\} \sim \{b_{\sigma,\tau}\}$ if

$$b_{\sigma,\tau} = \frac{k_\sigma \cdot \sigma(k_\tau)}{k_{\sigma\tau}} \cdot a_{\sigma,\tau} \quad (4.6)$$

Then $\sim$ is an equivalence relation on the set of factor sets.

Proof [Farb and Dennis, 2012][p: 118] ■

Definition 4.3: (Crossed Product Algebra) Let $\{k_{\sigma,\tau}\}$ be a factor set depending on $\mathbb{K}$, i.e. a subset of $\mathbb{K}$ which satisfies condition (4.5) of Theorem 4.2. The central simple $\mathbb{k}$ -algebra $\mathcal{A}$ corresponding to $\{k_{\sigma,\tau}\}$ satisfying Theorem 4.2 is called the crossed product algebra of $\mathbb{K}$ and G depending on $\{k_{\sigma,\tau}\}$. We denote it by

$$\mathcal{A} = (\mathbb{K}, G, k_{\sigma,\tau}) = \bigoplus_{\sigma \in G} \mathbb{K}.x_{\sigma} \quad (4.7)$$

The following result explores the relation between the crossed product algebras corresponding to equivalent factor sets.

Corollary 4.2: Let $\{a_{\sigma,\tau}\}$ and $\{b_{\sigma,\tau}\}$ be equivalent factor sets in the sense of Theorem 4.3. Then

$$(K, G, a_{\sigma,\tau}) \cong (K, G, b_{\sigma,\tau}) \quad (4.8)$$

Proof [Farb and Dennis, 2012] [p: 121] ■

Now we can turn back to Brauer groups and relate them to factor sets. Recall that elements of the relative Brauer group $\text{Br}(\mathbb{k}/\mathbb{K})$ are merely equivalence classes of central simple $\mathbb{k}$ -algebras which split over $\mathbb{K}$. We also built up the equivalence classes of factor sets depending on $\mathbb{K}$. As one might expect and as we will see these equivalence classes are in a one-to-one correspondence.

Theorem 4.4: Let $\mathbb{K}/\mathbb{k}$ be a Galois extension and G be a Galois group of $\mathbb{K}/\mathbb{k}$. Then, there is a one-to-one correspondence between equivalence classes of factor sets $\{k_{\alpha,\tau}\}$ depending on $\mathbb{K}$ and elements of $\text{Br}(\mathbb{K}/\mathbb{k})$.

Proof [Farb and Dennis, 2012] [p: 122] ■

4.2. Factor Sets and Galois Cohomology Groups

Definition 4.4: (n-cochain) Let G be any group and M be an abelian group. The n -th cochain group of the pair $\{G, M\}$ denoted by $C^n(G, M)$ is defined to be the set of all functions from G^n to M .

If $n = 0$ then $C^0(G, M) = M$. An element of $C^n(G, M)$ is also called an n -cochain of G with coefficients in M .

Note that for any abelian group $(M, +)$ and for any set X the set of functions from X to M is naturally an abelian group with pointwise addition. Explicitly for any functions $f, g : X \rightarrow M$, we set $f + g : X \rightarrow M$ as $(f + g)(x) = f(x) + g(x)$. The identity element is obviously the zero map, and the inverse of f is then $-f$. In particular we have the following fact.

Corollary 4.3: $C^n(G, M)$ is an abelian group under the pointwise addition.

In the rest of this section we suppose that the group G acts on M , i.e. there exists a map $G \times M \rightarrow M$ denoted by $(g, m) \mapsto g.m$ which satisfies

$$e_G.x = x \quad (4.9)$$

$$g_1.(g_2.x) = (g_1g_2).x \quad (4.10)$$

for all $g_1, g_2 \in G$ and $x \in M$ where e_G is the identity element of G .

Definition 4.5: The boundary maps $\{\delta_n\}_{n \geq 1}$ are the group homomorphism defined as follows;

$$\begin{aligned} \delta_n : C^n(G, M) &\longrightarrow C^{n+1}(G, M) \\ f \mapsto \delta_n(f)(g_1, g_2, \dots, g_{n+1}) &= g_1.(f(g_2, \dots, g_{n+1})) \\ &+ \sum_{i=1}^n (-1)^i f(g_1, \dots, g_{i-1}, g_i.g_{i+1}, \dots, g_{n+1}) \\ &+ (-1)^{n+1} f(g_1, \dots, g_n) \end{aligned} \quad (4.11)$$

For consistency we set $\delta_0(f)(g) = g.f - f$ for any $g \in G$ and $f \in C^0 = M$.

Example 4.1:

- i) $\delta_1(f)(g_1, g_2) = g_1f(g_2) - f(g_1g_2) + f(g_1)$, for $f \in C^1$.
- ii) $\delta_2(f)(g_1, g_2, g_3) = g_1f(g_2, g_3) - f(g_1g_2, g_3) + f(g_1, g_2g_3) - f(g_1, g_2)$, for $f \in C^2$.

Proposition 4.2: $\delta_{n+1} \circ \delta_n = 0$

Proof [Knapp, 2007b] [p: 358-359] ■

Definition 4.6: Within the notation of Definition 4.4 and Definition 4.5, the collection $\{C^n, \delta_n\}$ is called a cochain complex. We denote this cochain complex as

$$0 \longrightarrow C^0 \xrightarrow{\delta_0} C^1 \xrightarrow{\delta_1} \dots C^n \xrightarrow{\delta_n} C^{n+1} \xrightarrow{\delta_{n+1}} \dots \quad (4.12)$$

We set $Z^n = \text{Ker}(\delta_n)$ and $B^n = \text{Im}(\delta_{n-1})$ for $n \geq 1$. We put $B^0 = 0$. An element of Z^n is called an n -cocycle and an element of B^n is called an n -coboundary.

Definition 4.7: n -th cohomology group of G with coefficients in M is defined as follows:

$$H^n(G, M) = Z^n / B^n \quad (4.13)$$

If we take $G = \text{Gal}(\mathbb{K}/\mathbb{k})$ and $M = \mathbb{K}^*$ (as a multiplicative abelian group) for some Galois extension $\mathbb{K}/\mathbb{k}$, the group $H^n(\text{Gal}(\mathbb{K}/\mathbb{k}), \mathbb{K}^*)$ is called the n -th Galois cohomology group of the extension $\mathbb{K}/\mathbb{k}$.

Example 4.2: Let G and M be given as in Definition 4.4. We use multiplicative and additive notation for G and M respectively. We can easily compute Z^1 and B^1 . By definition we have that

$$\delta_1(f) \in C^2, \quad \delta_1(f)(g_1, g_2) = g_1 \cdot f(g_2) - f(g_1 g_2) + f(g_1) \quad (4.14)$$

So $f \in Z^1 = \text{Ker}(\delta_1)$ if and only if $f(g_1 g_2) = f(g_1) + g_1 \cdot f(g_2)$.

Now we consider $B^1 = \text{Im}(\delta_0)$. For any $m \in C^0 = M$, $\delta_0(f)(g) = g \cdot m - m$. So the image of δ_0 consists of the functions in C^1 which are of the form $g \mapsto g \cdot m - m$ for some fixed $m \in M$.

Now we restrict to trivial action of G on M , i.e. we set $g \cdot m = m$ for any $g \in G$ and $m \in M$. In this case $f \in Z^1 = \text{Ker}(\delta_1)$ if and only if $f(g_1 g_2) = f(g_1) + f(g_2)$, i.e. Z^1 is the group of group homomorphisms from G to M . Also in this case $\delta_0(f)(g) = g \cdot m - m = m - m = 0$, so that $B^1 = 0$. Therefore we see that $H^1(G, M) = Z^1$, i.e. $H^1(G, M) = \text{Hom}(G, M)$ where Hom means the set of group homomorphisms.

Example 4.3: Now we give a very simple example for $H^n = H^n(\text{Gal}(\mathbb{K}/\mathbb{k}), \mathbb{K}^*)$. Let $\mathbb{k} = \mathbb{Q}$ and $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, so that $\mathbb{K}/\mathbb{k}$ is a Galois extension with Galois group $G = \mathbb{Z}/2\mathbb{Z}$. Let's denote the elements of G by I and σ where I is the identity automorphism of $\mathbb{K}$ and $\sigma(\sqrt{2}) = -\sqrt{2}$. So G acts on $\mathbb{K}^*$ by $(\sigma_j, \alpha) \mapsto \sigma_j(\alpha)$. It is also convenient to use multiplicative notation for $\mathbb{K}^*$

By the preceding example $f \in Z^1 = \text{Ker}(\delta_1)$ if and only if

$$f(\sigma_i \sigma_j) = f(\sigma_i)(\sigma_i(f(\sigma_j))) \quad (4.15)$$

If we choose $\sigma_i = I$ and $\sigma_j = \sigma$ then we see that $f(I) = 1$. Also if we choose $\sigma_i = \sigma_j = \sigma$ we see that $f(\sigma) = -1$. Hence, we see that H^1 consists of one element, i.e. $H^1 = 0$.

Now, we examine the relation between factor sets and cohomology groups. By the paragraph preceding Lemma 4.1, we can associate a unique $\{x_\sigma\}$ to each $\sigma \in G$, which turns out to be a map $G \rightarrow \mathbb{K}^*$. In other words $\sigma \mapsto \{x_\sigma\}$ is a 1-cochain and $\{k_{\sigma,\tau}\}$ is a map $G \times G \rightarrow \mathbb{K}^*$. In the above terminology we may say that $\{x_\sigma\}$ is a 1-cochain and $\{k_{\sigma,\tau}\}$ is a 2-cochain by the Definition 4.4. We investigate this in more detail.

Lemma 4.2: An element of Z^2 is a factor set.

Proof [Farb and Dennis, 2012][p: 125] Elements of Z^2 are functions from $G \times G$ to $\mathbb{K}^*$. Then there exists $a \in Z^2$ for any $\rho, \sigma, \tau \in G$ such that the following hold:

$$1 = \delta_2(a)(\rho, \sigma, \tau) \quad (4.16)$$

Then,

$$1 = \rho(a(\sigma, \tau))a(\rho\sigma, \tau)^{-1}.a(\rho, \sigma\tau).a(\rho, \sigma)^{-1} \quad (4.17)$$

$$\rho(a(\sigma, \tau))a(\rho, \sigma\tau) = a(\rho\sigma, \tau).a(\rho, \sigma) \quad (4.18)$$

$a(\sigma, \tau), a(\rho\sigma, \tau), a(\rho, \sigma\tau)$ are elements of $\mathbb{K}^*$. If we replace $k_{\sigma,\tau}, k_{\rho\sigma,\tau}, k_{\rho,\sigma\tau}$ in Theorem 4.2 by $a(\sigma, \tau), a(\rho\sigma, \tau), a(\rho, \sigma\tau)$, we see that Equation (4.18) is the same as condition (4.5) of Theorem 4.2. Therefore the 2-cocycles in $C^2(G, \mathbb{K}^*)$ are factor sets relative to $\mathbb{K}^*$.

Now let's look at the relation between these elements and the elements of B^2 . Element of B^2 is $\text{Im}(\delta_1(f))$ where $f : G \rightarrow \mathbb{K}^*$. i.e.

$$\delta_1(f)(\sigma, \tau) = \sigma(f(\tau))f(\sigma\tau)^{-1}f(\sigma) = \frac{\sigma(f(\tau))f(\sigma)}{f(\sigma\tau)} \quad (4.19)$$

Since $B^2 \subset Z^2$, $\delta_1(f)(\sigma, \tau)$ is a factor set relative to $\mathbb{K}^*$. Then we can find 1-cochain f for $a \sim b$ in Z^2 such that:

$$b(\sigma, \tau) = \delta_1(f)(\sigma, \tau) \cdot a(\sigma, \tau) \quad (4.20)$$

Then,

$$b(\sigma, \tau) = \frac{\sigma(f(\tau))f(\sigma)}{f(\sigma\tau)} a(\sigma, \tau) \quad (4.21)$$

In a similar way, we can replace $a_{\sigma,\tau}, b_{\sigma,\tau}, k_{\sigma\tau}, k_\tau, k_\sigma$ in Theorem 4.3 by $a(\sigma, \tau), b(\sigma, \tau), f(\sigma\tau), f(\tau), f(\sigma)$ respectively. Then Equation (4.21) is the same as condition (4.6) of Theorem 4.3. ■

We previously saw that there is a one-to-one and onto correspondence between $Br(\mathbb{K}/\mathbb{k})$ and the set of factor sets by the Theorem 4.4. Now we have found a one-to-one onto correspondence between factor sets and $H^2(G, \mathbb{K}^*)$. So we have a one-to-one correspondence between $Br(\mathbb{K}/\mathbb{k})$ and $H^2(G, \mathbb{K}^*)$. Now let's see that this is indeed an isomorphism. The only thing left to reach this conclusion is to find a well-defined map. The next theorem adressess this point.

Theorem 4.5: Let $\mathbb{K}/\mathbb{k}$ be a Galois extension with the Galois group group G and $a = \{u_{\sigma,\tau}\}$ and $b = \{v_{\sigma,\tau}\}$ be two factor sets. Then

$$[(\mathbb{K}, G, a)] \cdot [(\mathbb{K}, G, b)] = [(\mathbb{K}, G, a.b)] \quad (4.22)$$

Proof [Farb and Dennis, 2012] [p: 126-128] ■

After the Theorem 4.5, the following two corollaries can be obtained easily.

Corollary 4.4: Let $\mathbb{K}/\mathbb{k}$ be a finite Galois field extension, with Galois group G . Then

$$H^2(G, \mathbb{K}^*) \cong Br(\mathbb{K}/\mathbb{k}) \quad (4.23)$$

Proof Let we define a map ψ as follows:

$$\begin{aligned} \varphi : H^2(G, \mathbb{K}^*) &\longrightarrow Br(\mathbb{K}/\mathbb{k}) \\ a &\longrightarrow [(\mathbb{K}, G, a)] \end{aligned} \quad (4.24)$$

From the Theorem 4.4 this map is one to one and onto. By the above Theorem 4.5 we know this map is a group homomorphism. Therefore φ is an isomorphism. ■

Corollary 4.5:

$$Br(\mathbb{k}) \cong \bigcup_K H^2(Gal(\mathbb{K}/\mathbb{k}), \mathbb{K}^*) \quad (4.25)$$

Proof By using the Theorem 3.8 and the Theorem 4.4 together, we can easily obtain the result. ■

5. BRAUER - MANIN OBSTRUCTION

We gave most of definitions required for Brauer-Manin obstruction. Now we will give some important definitions and theorems in the last part.

5.1. Ring Of Adeles

As we know from the Hasse principle, a quadratic form has a solution in rational numbers if and only if it has a solution in real numbers and $\mathbb{Q}_p$ for all prime p . We can use the ring of adeles for the solutions over $\mathbb{Q}_p$ and $\mathbb{R}(= \mathbb{Q}_\infty)$.

Definition 5.1: (Ring of Adeles) The ring of Adeles of rational numbers is defined as $\mathbb{A}_\mathbb{Q} := \mathbb{R} \times (\prod_{p \in S} \mathbb{Q}_p) \times (\prod_{p \notin S} \mathbb{Z}_p)$ where S is any finite subset of prime numbers. Variety of adelic spaces denoted $V(\mathbb{A}_\mathbb{Q}) := \{(a_p) | a_p \in V(\mathbb{Q}_p)\}$.

An element of the ring of adeles is an infinite tuple such that every coordinate are from p -adic numbers and integers. Then every coordinate of a variety of adelic spaces is a p -adic solution or real solution.

5.2. Obstruction

First of all, we will define the maps i, Ψ_A, Φ_A to use in the main theorem. We can convert any rational number to a p -adic number via constant sequence. Then we have a canonical map $\mu_p : \mathbb{Q} \rightarrow \mathbb{Q}_p$ for each p defined as follows:

$$\mu_p : \mathbb{Q} \longrightarrow \mathbb{Q}_p \tag{5.1}$$

$$r \longmapsto \{r, r, \dots\}$$

Let $V(\mathbb{Q})$ be a variety over $\mathbb{Q}$ given by the ideal I in $\mathbb{Q}[x_1, \dots, x_n]$ and $\mathcal{R}$ be the quotient ring $\mathbb{K}[x_1, \dots, x_n]/\sqrt{I}$. With the above map, we can define a map from $V(\mathbb{Q})$ to $V(\mathbb{A}_\mathbb{Q})$ as follows:

$$i : V(\mathbb{Q}) \longrightarrow V(\mathbb{A}_\mathbb{Q}) \tag{5.2}$$

$$x \longmapsto \{x, \mu_2(x), \mu_3(x) \dots\}$$

Elements of $\mathcal{R}$ are equivalence classes of polynomials. Then for any $x \in V(\mathbb{Q})$, we have an induced map as follows:

$$\begin{aligned}\psi_x : \mathcal{R} &\longrightarrow \mathbb{Q} \\ f &\longmapsto f(x)\end{aligned}\tag{5.3}$$

So we can see $\mathbb{Q}$ as an $\mathcal{R}$ -algebra via this map depending on x . Applying $Br(\cdot)$, we obtain a map $Br(\psi_x) : Br(V) \rightarrow Br(\mathbb{Q})$. Hence, we have a map $\Psi : V(\mathbb{Q}) \times Br(V) \rightarrow Br(\mathbb{Q}_p)$. If we fix $\mathcal{A} \in Br(V)$, we obtain:

$$\begin{aligned}\Psi_{\mathcal{A}} =: V(\mathbb{Q}) &\longrightarrow Br(\mathbb{Q}) \\ (x) &\longrightarrow [\mathcal{A} \otimes_R \mathbb{Q}]\end{aligned}\tag{5.4}$$

Similarly, we can define a map $\Phi_{\mathcal{A}}$ for a fixed $[\mathcal{A}] \in Br(V)$ as follows:

$$\begin{aligned}\Phi_{\mathcal{A}} =: V(A_{\mathbb{Q}}) &\longrightarrow \bigoplus_p Br(\mathbb{Q}_p) \\ (x_p) &\longrightarrow \sum_p [\mathcal{A} \otimes_R \mathbb{Q}_p]\end{aligned}\tag{5.5}$$

The next two theorems are very important for this work but we give them without proof. These theorems are central in class field theory and the reader can refer to [Web 7, 2020] for further details.

Theorem 5.1: There exists an isomorphism

$$\text{inv}_p : Br(\mathbb{Q}_p) \rightarrow \mathbb{Q}/\mathbb{Z}\tag{5.6}$$

Proof [Web 7, 2020] [p: 141] ■

Theorem 5.2: The following is a short exact sequence.

$$0 \rightarrow Br(\mathbb{Q}) \rightarrow \bigoplus_p Br(\mathbb{Q}_p) \xrightarrow{\sum_p \text{inv}_p} \mathbb{Q}/\mathbb{Z} \rightarrow 0\tag{5.7}$$

Proof [Web 7, 2020] [p: 241] ■

We will use the invariant map to just talk about isomorphism in this work. The Corollary 2.5 and the Theorem 2.21 will be used for the computation of obstruction.

We have a quaternion algebra $\left(\frac{\alpha, \beta}{\mathbb{Q}_p}\right)$ for any $\alpha, \beta \in \mathbb{Q}_p$. If $(\alpha, \beta)_p = 1$ then $\left[\left(\frac{\alpha, \beta}{\mathbb{Q}_p}\right)\right]$ is the identity element of $Br(\mathbb{Q}_p)$ since $\left(\frac{\alpha, \beta}{\mathbb{Q}_p}\right)$ is isomorphic to matrix algebra $M_2(\mathbb{Q}_p)$ by Corollary 2.5. Then $\text{inv}_p(M_2(\mathbb{Q}_p)) = 0$. Similarly if $(\alpha, \beta)_p = -1$, then $\text{inv}_p\left(\left(\frac{\alpha, \beta}{\mathbb{Q}_p}\right)\right) \neq 0$. For the last theorem, we are interested in whether the result of the invariant map is 0 or not.

Definition 5.2: Let $[\mathcal{A}] \in Br(V)$. We define

$$V(A_{\mathbb{Q}})^{\mathcal{A}} := \{(x_p) \in A_{\mathbb{Q}} : \sum_p \text{inv}_p \Phi_{\mathcal{A}}(x_p) = 0\} \quad (5.8)$$

$$V(A_{\mathbb{Q}})^{Br} := \bigcap_{[\mathcal{A}] \in Br(V)} V(A_{\mathbb{Q}})^{\mathcal{A}} \quad (5.9)$$

$V(A_{\mathbb{Q}})^{Br}$ is called a *Brauer-Manin set*.

It is clear that $V(A_{\mathbb{Q}})^{Br} \subset V(A_{\mathbb{Q}})$ by the Definition 5.2. We must show $V(\mathbb{Q}) \subset V(A_{\mathbb{Q}})^{Br}$ for the obstruction. The next theorem is the main theorem that was proved by Yuri Manin. [Manin, 1971]

Theorem 5.3: $V(\mathbb{Q}) \subset V(A_{\mathbb{Q}})^{Br}$

Proof Let $[\mathcal{A}] \in Br(V)$. We have the following diagram where i is injective.

$$\begin{array}{ccccccc} V(\mathbb{Q}) & \xrightarrow{i} & V(\mathbb{A}_{\mathbb{Q}}) & & & & \\ \downarrow \Psi_{\mathcal{A}} & & \downarrow \Phi_{\mathcal{A}} & & & & \\ 0 & \longrightarrow & Br(\mathbb{Q}) & \xrightarrow{j} & \bigoplus_p Br(\mathbb{Q}_p) & \xrightarrow{\sum_p \text{inv}_p} & \mathbb{Q}/\mathbb{Z} \longrightarrow 0 \end{array} \quad (5.10)$$

By functionality of $Br(\cdot)$ the above diagram is commutative, i.e.

$$\Rightarrow \Phi_{\mathcal{A}} \circ i = j \circ \Psi_{\mathcal{A}}$$

$$\Rightarrow (\sum_p \text{inv}_p) \circ \Phi_{\mathcal{A}} \circ i = (\sum_p \text{inv}_p) \circ j \circ \Psi_{\mathcal{A}} = \underbrace{((\sum_p \text{inv}_p) \circ j)}_0 \circ \Psi_{\mathcal{A}} = 0$$

$$\Rightarrow (\sum_p \text{inv}_p) \circ \Phi_{\mathcal{A}} \circ i(x) = 0 \text{ for all } \mathcal{A} \in Br(V) \text{ and } x \in V(\mathbb{Q})$$

$$\Rightarrow x \in V(\mathbb{A}_{\mathbb{Q}})^{Br} \text{ for all } x \in V(\mathbb{Q})$$

■

So we reach $V(\mathbb{Q}) \subset V(A_{\mathbb{Q}})^{Br} \subset V(A_{\mathbb{Q}})$. The Hasse principle says briefly that if $V(A_{\mathbb{Q}}) \neq \emptyset$ then $V(\mathbb{Q}) \neq \emptyset$ for the quadratic forms. But for some variety of non-quadratic forms, it is possible to be $V(A_{\mathbb{Q}})^{Br} = \emptyset$ while $V(A_{\mathbb{Q}}) \neq \emptyset$. In this case, $V(\mathbb{Q})$ must be an empty set. This is what we call as the Brauer-Manin obstruction to the Hasse principle.

5.3. Example

In this section, we will give a well-known example of Brauer-Manin obstruction.

Example 5.1: [Web 5, 2020] Consider the equation be $2y^2 = x^4 - 17 \neq 0$. This equation has a nontrivial solution in $\mathbb{Q}_p$ for all p but has no nontrivial rational solution. Now, we explain it.

We can extend the quaternion algebra $\left(\frac{y, 17}{\mathbb{Q}_p}\right)$ to the quaternion algebra $A = \left(\frac{y, 17}{V}\right)$.

Let $\mathcal{A} = \left(\frac{y, 17}{V}\right) \in Br(V)$ and $(x_p) \in V(A_{\mathbb{Q}})$, then

- *If $p \neq 17$, then $\text{inv}_p \Phi_{\mathcal{A}}(x_p) = 0$*
- *If $p = 17$, then $\text{inv}_p \Phi_{\mathcal{A}}(x_p) \neq 0$*

$V(A_{\mathbb{Q}})^A = \emptyset$ since $\sum_p \text{inv}_p \Phi_{\mathcal{A}}(x_p) \neq 0$ for all $(x_p) \in V(A_{\mathbb{Q}})$. Then $V(A_{\mathbb{Q}})^{Br} = \emptyset$. Therefore $V(\mathbb{Q}) = \emptyset$.

6. CONCLUSION

In this thesis, we studied how Brauer-Manin obstruction explains the failure of the Hasse principle for some varieties given by nonquadratic polynomials. Even the Brauer-Manin obstruction is a powerful and deep theory, it is far from being a complete obstruction to the Hasse principle. This work can be continued with recent refinements of Brauer-Manin obstruction.

REFERENCES

- Aitken W., Lemmermeyer F., (2011), “Counterexamples to the Hasse principle”, The American Mathematical Monthly, 118(7), 610-628.
- Atiyah M., (1994), “Introduction to Commutative Algebra”, 1th Edition, CRC Press.
- Auslander M., Goldman O., (1960), “The Brauer Group of a Commutative Ring”, Trans. Amer. Math. Soc., 97 , 367-409.
- Borevich Z. I. , Shafarevich I. R., (1986), “Number Theory ”, 1st Edition, Academic Press.
- Brešar M., (2014), “Introduction to Noncommutative Algebra ”, 1st Edition, Springer.
- Chen H., (2019), “The Brauer Group of Rational Numbers”, arXiv preprint arXiv:1911.02368.
- Çallıalp F., Tekir Ü., (2009), “Değişmeli Halkalar ve Modüller ”, 1st Edition, Birsan Yayınevi.
- DeMeyer F. , Ingraham E., (1971), “Separable Algebras Over Commutative Rings”, 1st Edition, Springer.
- Drensky V., Giambruno A., Sehgal S. K. (Eds.), (1998), “Methods in Ring Theory ”, 1st Edition, CRC Press.
- Dummit D. S., Foote R. M., (2004), “Abstract Algebra ”, 3st Edition, Hoboken: Wiley.
- Farb B., Dennis R. K., (2012), “Noncommutative Algebra ”, 1st Edition, Springer Science & Business Media.
- Flynn E.V., (2004), “The Hasse Principal and the Brauer-Manin Obstruction for Curves”, Manuscripta Math., 115, 437 - 466.
- Herstein I. N., (1994), “Noncommutative Rings ”, 1st Edition, American Mathematical Soc.
- Hartshorne R., (1997), “Graduate Text in Mathematics: Algebraic Geometry”, 1st Edition, Springer-Verlag.
- Karakaş H. İ., (2008), “Cebir Dersleri”, 1st Edition, Türkiye Bilimler Akademisi.
- Knapp A. W., (2007a), “Advanced Algebra”, 1st Edition, Springer Science & Business Media.
- Knapp A. W., (2007b), “Basic Algebra”, 1st Edition, Springer Science & Business Media.
- Lang S., (2004), “Algebra”, 3st Edition, Inventiones Mathematicae, Graduate Texts in Mathematics.

- Lerner B., (2007), “The Brauer-Manin Obstruction to the Hasse Principle ”, Master Thesis, The University of New South Wales.
- Lind C. E., (1940), “Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins”, Appelberg.
- Manin Y. I., Panchishkin A. A., (2005), “Introduction to Modern Number Theory”, 2st Edition, Springer.
- Manin, Y. I., (1971), “Le Groupe de Brauer–Grothendieck en Géométrie Diophantienne”, Actes du Congrès International des Mathématiciens, Gauthier-Villars, Paris, 1971, 401–411.
- Mazur B., (1993), “On the Passage From Local to Global in Number Theory”, Bulletin of the American Mathematical Society, 29(1), 14-50.
- Niven I. , Zuckerman H. S., Montgomery H. L., (1991), “An Introduction to the Theory of Numbers”, 5th edition, John Wiley & Sons.
- Poonen B., (2010), “Insufficiency of the Brauer-Manin Obstruction Applied to Étale Covers”, Annals of Mathematics, 2157-2169.
- Reichardt H., (1942), “Einige im Kleinen überall lösbare, im Großen unlösbare diophantische Gleichungen”, Journal für die reine und angewandte Mathematik, 1942(184), 12-18.
- Robert E. P., (2009) , “The Brauer-Manin Obstruction and the Hasse Principle”, Master Thesis, University of New Brunswick.
- Rowen L. , Saltman D. J., (2013), “Tensor Products of Division Algebras and Fields”, Journal of Algebra, 394, 296-309.
- Selmer E. S., (1951), “The Diophantine Equation $x^3 + y^3 + z^3 = 0$ ”, Acta Mathematica, 85(1), 203-362.
- Serre J. P., (2012), “A Course in Arithmetic ”, 1th Edition, Springer Science & Business Media.
- Skorobogatov A.N., (1999), “Beyond the Manin Obstruction ”, Inventiones Mathematicae, Springer 135, 2- 399-424.
- Skorobogatov A.N. , Zarhin Y.G., (2008), “A finiteness Theorem for the Brauer Group of Abelian Varieties and K3 Surfaces”, J. Alg. Geom., 17, 481–502.
- Ueno K., (1999), “Algebraic Geometry 1. From Algebraic Varieties to Schemes”, 1th Edition, Transl. Math.
- Voight J., (2020) “Quaternion Algebras”, 1th Edition, Springer.
- Web 1, (2019), <http://math.uchicago.edu/~may/REU2019/REUPapers/Wang,Xingyu.pdf> , (Date of Access: 21/10/2019).
- Web 2, (2019), <https://www.jmilne.org/math/CourseNotes/AG.pdf> , (Date of Access: 10/04/2019).

Web 3, (2019), <https://kconrad.math.uconn.edu/math5211s13/handouts/tensorprod.pdf> , (Date of Access: 13/12/2019).

Web 4, (2020), <http://www.fen.bilkent.edu.tr/franz/ag05/ag-02.pdf> , (Date of Access: 01/03/2020).

Web 5, (2020), <https://www.math.arizona.edu/swc/aws/2015/2015Colliot-TheleneNotes.pdf> , (Date of Access: 02/04/2020).

Web 6, (2020), <https://math.berkeley.edu/shellym/BrauerManin.pdf> , (Date of Access: 17/05/2020).

Web 7, (2020), <https://www.jmilne.org/math/CourseNotes/CFT.pdf> , (Date of Access: 23/01/2020).

Web 8, (2020), <http://personal.psu.edu/mup17/Research/Gross.pdf> , (Date of Access: 07/10/2020).

BIOGRAPHY

Oktaý CESUR was born in Düzcce, Turkey in 1988. He graduated from Çanakkale Onsekiz Mart University, Department of Mathematics in 2013. He started his master's degree Gebze Technical Universty in 2018. Completed his master's degree in Gebze Technical University Mathematics. Also, he has been working as a teacher since 2013. His area of interest is algebra and computer science.

APPENDICES

Appendix : Publications

Cesur O., “Hasse Principle and Brauer-Manin Obstruction”, 3rd International E-Conference on Mathematical Advances and Applications, 24-06-2020, Istanbul, Turkey.