HASSE-MINKOWSKI PRINCIPLE FOR QUADRATIC FORMS OVER $\mathbb{Q}$

Hardik Tankaria

Supervisor- Dr. Narasimha Kumar

A Thesis Submitted to
Indian Institute of Technology Hyderabad
In Partial Fulfillment of the Requirements for The Degree of Master of Science in
Mathematics

भारतीय प्रौद्योगिकी संस्थान हैदराबाद
Indian Institute of Technology Hyderabad

Department of Mathematics
May 2016

Declaration

I declare that this written submission represents my ideas in my own words, and where ideas or words of others have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea,data,fact and source in my submission. I understand that any violation of the above will be a cause for disciplinary action by the Institute and can also evoke penal action from the sources that have thus not been properly cited, or from whom proper permission has not been taken when needed.

H. D. Tankaria

Hardik Tankaria

Roll No. MA14MSCST11008

Approval Sheet

This Thesis entitled **Hasse-Minkowski priciple for quadratic forms over $\mathbb{Q}$** by Hardik Tankaria is approved for the degree of Master of Science from Indian Institute of Technology Hyderabad.

CH.V.G.N. Kumar
Dr. Narasimha Kumar 03/05/16.
(Supervisor)
Department of Mathematics
Indian Institute of Technology Hyderabad

Acknowledgments

First and foremost I want to thank my advisor Dr. Narasimha Kumar. It has been an honor to be his second student. He has taught me consciously. I appreciate all his contributions of time, ideas, and to make my M.Sc. project experience productive. The joy and enthusiasm he has for his research was contagious and motivational for me, even during tough times in the M.Sc. I am also thankful for the excellent examples he has provided as a successful professor.

I would like to acknowledge the help of Mr. Surjeet Kaushik, a semester ago. We worked together in my first part of thesis and I very much appreciated his enthusiasm, intensity, willingness to contribute to this work. I thank Dr. Pradipto Banerjee for the helpful discussion.

The time spent at Indian Institute of Technology Hyderabad was made enjoyable in large part due to the many friends and groups that became a part of my life. I am grateful for time spent with classmates and friends, for my backpacking buddies and our memorable trips into the mountains, and for many other people and memories.

Lastly, I would like to thank my parents and family for all their love and encouragement. Especially, my **parents** who raised me with a love of mathematics and supported me in all my pursuits.

Hardik Tankaria,
Indian Institute of Technology Hyderabad,
May 2016.

Abstract

I have greatly benefited reading a book of Serre [Ser73], and I have presented a detailed version of the main results in this book.

One of the main interesting topic in algebra is to find the roots of non-zero polynomials and writing down them explicitly over a given field $\mathbb{K}$. The case which we consider in this project is the space of quadratic forms, which are homogeneous polynomials of degree 2, over $\mathbb{Q}$. If they arise over $\mathbb{Z}$, then we can study the zeros of these quadratic form by looking at them over $\mathbb{Z}_p$ and study if that has zero in $\mathbb{Z}_p$ or not. By Hensels lemma, this studied over the reduction modulo p.

Then immediately question arise is to study if the quadratic form represents a value or not, over $\mathbb{Q}_p$. By studying the structure of the group $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, one can understand this question and bring it to a finite representation problem.

The next question arise that when quadratic forms represents zero. Hasse-Minkowski principle answers that question. Hasse-Minkowski principle says that quadratic forms Q has a global zero if and only Q has everywhere a local zero. This means that if Q is a quadratic form over $\mathbb{Q}$, Q represents zero, it is necessary and sufficient that, for all $v \in V$, the form Q_v represent zero $\mathbb{Q}_v$, where V is finite set of primes including ∞ and 2. For that we study non-degenerate quadratic module over field $\mathbb{K}$ and by Hilbert symbol we give product formula which is the one most important invariant of the quadratic form.

Generally, we are concentrating on equivalence of two quadratic forms, because two quadratic forms are equivalent if and only if they have same rank and same discriminant and same invariant ϵ, so that by equivalence we can consider one of them over $\mathbb{Q}_p$ and can apply Hasse-Minkowski principle on it. This invariants discriminant, rank and ϵ are called local invariants of Q. Similarly, we can do this for any element a belong in to field $\mathbb{Q}^*$, this means Q represents a, it is necessary and sufficient that it does in each of the $\mathbb{Q}_p$. As an application of Hasse-Minkowski principle, we prove that a quadratic form of rank greater or equal to 5 represents zero if and only if it is indefinite, which means if it represents zero in $\mathbb{R}$.

I have greatly benefited reading a book of Serre [Ser73,], and I have presented a detailed version of the main results from that book in this thesis.

Notation

$\mathbb{N}$	Set of all natural numbers
$\mathbb{Z}$	Set of all integers
$\mathbb{Q}$	Set of all rational numbers
$\mathbb{R}$	Set of all real numbers
$\mathbb{C}$	Set of all complex numbers
$\mathbb{Z}/p\mathbb{Z}$	Ring of integers modulo p
$\mathbb{Z}/p^n\mathbb{Z}$	Ring of integers modulo p^n
R^*	Set of all invertible elements in the ring R
$\mathbb{F}$ or $\mathbb{K}$	Fields
$\#A$	Cardinality of set A
$\mathrm{char}\, R$	Characteristic of R
$\ker \varphi$	Kernel of homomorphism of φ
$\deg f(x)$	Degree of polynomial $f(x)$
$\mathbb{F}(a_1, a_2, \ldots, a_n)$	Extension of $\mathbb{F}$ by $\{a_1, a_2, \ldots, a_n\}$
$[\mathbb{K} : \mathbb{F}]$	Degree of $\mathbb{K}$ over $\mathbb{F}$
$\mathbb{F}^n$	n-copies of field $\mathbb{F}$
$\dim_{\mathbb{F}} \mathbb{K}$	Dimension of vector space $\mathbb{K}$ over $\mathbb{F}$
$\mathbb{F}_q$	Field $\mathbb{F}$ with q elements, q is a power of prime
$\mathbb{Z}_p$	Ring of p-adic integers
$\mathbb{Q}_p$	Field of p-adic numbers
$R[x]$	Polynomial ring of R
$\varprojlim$	Inverse or projective limit of projective system
U	Group of invertible elements of $\mathbb{Z}_p$
$\nu_p(x)$	p-adic valuation of x

Contents

This thesis is dedicated to my parents for their endless Love, Encouragement, and Belief.

Chapter 1

Finite Fields

All rings considered below are to be commutative ring with unity. Ring homomorphism are always assumed to take unit element to unit element.

1.1 Generalities

In this section we will see basic structural results of finite fields, and later we will prove that multiplicative groups of finite field are cyclic.

1.1.1 Finite Fields

Definition 1 (Field)**.** *A commutative ring R with unity $1(\neq 0)$ in which every non-zero element has an inverse with respect to multiplication is called a field.*

Definition 2 (Finite field)**.** *A field with finite number of elements is called a finite field.*

Proposition 1.1.1. *If R is a ring, then $\exists!$ ring homomorphism $\varphi \colon \mathbb{Z} \to R$.*

Proof. Define $\varphi \colon \mathbb{Z} \to R$ by

$$\varphi(n) = \begin{cases} \underbrace{1_R + 1_R + \cdots + 1_R}_{n-times} & \text{if } n > 0, \\ 0 & \text{if } n = 0, \\ -\varphi(-n) & \text{if } n < 0. \end{cases}$$

Its clear that, for any $m, n \in \mathbb{Z}$, $\varphi(m+n) = \varphi(m) + \varphi(n)$ and $\varphi(mn) = \varphi(m)\varphi(n)$. □

The proposition above allows us to identify the image of an integer in an arbitrary ring R. For ex. 4 can be interpreted by $1_R + 1_R + 1_R + 1_R$ of R.

Proposition 1.1.2. *Let $\mathbb{K}$ be a field and $\varphi\colon \mathbb{Z} \to \mathbb{K}$ be homomorphism then $\varphi(\mathbb{Z})$ is a subring of $\mathbb{K}$.*

Proof. $\varphi(\mathbb{Z}) = \{\varphi(z)\colon z \in \mathbb{Z}\}$. Let $a, b \in \mathbb{K}$ then $\varphi(z_1) = a$ and $\varphi(z_2) = b$ for some $z_1, z_2 \in \mathbb{Z}$. Then $a - b = \varphi(z_1) - \varphi(z_2) = \varphi(z_1 - z_2) \in \mathbb{K}$, also $ab = \varphi(z_1)\varphi(z_2) = \varphi(z_1 z_2) \in \mathbb{K}$. So, $\varphi(\mathbb{Z})$ is subring of $\mathbb{K}$. □

Lemma 1.1.3. *$\mathbb{Z}/n\mathbb{Z}$ is integral domain if and only if n is prime number.*

Proof. Let n is prime, consider $\overline{x}(\neq 0) \in \mathbb{Z}/n\mathbb{Z}$ then we can choose $a \in \mathbb{Z}$ such that $2 \leq a \leq n-1$ with $\overline{a} = \overline{x}$. Since n is prime $(a, n) = 1$. Then $\exists\, r, m \in \mathbb{Z}$ such that $ar + mn = 1 \Rightarrow ra \equiv 1 \pmod{n}$. So $\overline{r}\,\overline{a} = 1$ in $\mathbb{Z}/n\mathbb{Z}$. Then $\overline{a}$ is unit in $\mathbb{Z}/n\mathbb{Z}$. So $\mathbb{Z}/n\mathbb{Z}$ is field and every field is integral domain. Now $\mathbb{Z}/n\mathbb{Z}$ is integral domain. If n is not prime number, then $n = ab$ with $a, b \in \mathbb{Z}$, also $a \neq 0, b \neq 0$ but $\overline{a} \cdot \overline{b} = \overline{n} = 0$ and $\mathbb{Z}/n\mathbb{Z}$ is integral domain. So n has to be prime. □

Definition 3 (Characteristic of field)**.** *Characteristic of field $\mathbb{K}$ is defined to be smallest positive integer p such that $p \cdot 1_{\mathbb{K}} = 0$. If such p exists otherwise it is zero. It is denoted by Char$(\mathbb{K})$.*

Proposition 1.1.4. *Characteristic of a field $\mathbb{F}$ is either 0 or a prime number.*

Proof. Suppose that the characteristic is not prime $p \neq 0$. So p is the smallest natural number such that $p.1 = 0$ in $\mathbb{F}$. Since p is not prime $p = rs$ is composite, $1 < r, s < p$ for $r, s \in \mathbb{Z}$, we have $r.1$ and $s.1$ are non-zero in $\mathbb{F}$ but $(r.1)(s.1) = (rs).1 = p.1 = 0$. Hence, $r.1$ is a non-zero zero divisor in field $\mathbb{F}$, which is a contradiction. This implies that p is prime number. □

Definition 4 (Field of fractions)**.** *The field of fractions of integral domain R, denoted $Q(R) = R \times R^*$ (where R^* is non-zero elements of R) is the set of equivalence classes, under the equivalence relation $\sim$ defined $(a, b) \sim (c, d)$ if and only if $ad = bc$. Given two elements $[a, b]$ and $[c, d]$ define $[a, b] + [c, d] = [ad + bc, bd]$ and $[a, b][c, d] = [ab, cd]$.*

Proposition 1.1.5. *Any field have only zero and unit ideals.*

Proof. Since every field have zero ideal, and in field every non-zero element has multiplicative inverse. So that ideal I contains unity 1. i.e., Field have only zero ideal and other one is whole ring R. □

Proposition 1.1.6. *Every homomorphism φ from field $\mathbb{F}$ to ring R is injective.*

Proof. We know that $\ker\varphi$ is an ideal of $\mathbb{F}$. Then by previous proposition $\ker\varphi$ is (1) or (0). If $\ker\varphi$ is (1) then map φ will zero map and zero map is not homomorphism when ring is not zero ring. So $\ker\varphi = \{0\}$, but if $\ker\varphi = \{0\}$ then φ is injective. Let $\ker\varphi = \{0\}$ and $x, y \in \mathbb{F}$, $\varphi(x) = \varphi(y) \Rightarrow \varphi(x) - \varphi(y) = 0 \Rightarrow \varphi(x-y) = 0 \Rightarrow x-y \in \ker\varphi \Rightarrow x-y = 0 \Rightarrow x = y$. Hence, φ is injective. □

Proposition 1.1.7. *Every field $\mathbb{F}$ contains either a copy of $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p.*

Proof. Field $\mathbb{F}$ is a ring with unity and from Proposition 1.1.4 characteristic of $\mathbb{F}$ is either prime $p > 0$ or zero. From Proposition 1.1.2 map $\varphi : \mathbb{Z} \to \mathbb{F}$ ring homomorphism. If characteristic is prime p, then $\ker \varphi = p\mathbb{Z}$. Since $\varphi(\mathbb{Z})$ is subring of field $\mathbb{F}$. By first isomorphism theorem of ring, $\varphi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$, but $\mathbb{Z}/p\mathbb{Z}$ is field. Then $\varphi(\mathbb{Z})$ is subfield of $\mathbb{F}$. Hence field $\mathbb{F}$ contains isomorphic copy of $\mathbb{Z}/p\mathbb{Z}$. Now assume that characteristic of field $\mathbb{F}$ is zero. We know that the intersection $\mathbb{F}_0$ of all subfields of $\mathbb{F}$ is again a field-called the prime subfield of $\mathbb{F}$. It is the smallest subfield of $\mathbb{F}$. The prime subfield must contain 1 and all its multiples $n \cdot 1$. From Proposition 1.1.2 map $\varphi : \mathbb{Z} \to \mathbb{F}$ is ring homomorphism. Its image must be contained in $\mathbb{F}_0$. If the kernel of this homomorphism is $\{0\}$, then by first isomorphism theorem of ring $\mathbb{F}_0$ contains a subring isomorphic to $\mathbb{Z}$, and hence it contains a subfield isomorphic to the field of fractions $\mathbb{Q}$ of $\mathbb{Z}$. By minimality, $\mathbb{F}_0 \cong \mathbb{Q}$. Hence, $\mathbb{F}$ contains isomorphic copy of $\mathbb{Q}$. □

Definition 5 (Subfield). *A subset $\mathbb{K}$ of field $\mathbb{F}$ is subfield if $\mathbb{K}$ itself is field respect to the operations of $\mathbb{F}$.*

Definition 6 (Finite field order). *Number of elements in finite field is called its order.*

Proposition 1.1.8. *If characteristic of field $\mathbb{K}$ is p then $\sigma \colon x \to x^p$ is an isomorphism of $\mathbb{K}$ onto one of its subfield $\mathbb{K}^p$.*

Proof. By definition, $\mathbb{K}^p := \{k^p | k \in \mathbb{K}\}$ is a field and $\#\mathbb{K}^p = \#\mathbb{K}$. We have
$\sigma(xy) = (xy)^p = x^p y^p = \sigma(x)\sigma(y)$ and $\sigma(x+y) = (x+y)^p$

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1}y + \binom{p}{2} x^{p-2}y^2 + \ldots + \binom{p}{p-1} xy^{p-1} + y^p$$

Since $\binom{p}{a} \equiv 0 \pmod{p}$, if $0 < a < p$. Say $\binom{p}{r} = tp$ $\binom{p}{r} x^{p-r}y^r = tpx^{p-r}y^r = t(0) = 0$ for
$0 < r < p \Rightarrow \sigma(x+y) = (x+y)^p = x^p + y^p = \sigma(x) + \sigma(y)$. So σ is homomorphism.
Now, let us show that σ is injective. If $x, y \in \mathbb{K}$ such that $\sigma(x) = \sigma(y)$. This implies that $x^p = y^p$ $= x^p - y^p = 0$, but $\sigma(x - y) = (x-y)^p = x^p - y^p = \sigma(x) - \sigma(y) = x^p - y^p = 0 \Rightarrow x = y$. So σ is injective. Since, $\#\mathbb{K} = \#\mathbb{K}^p$. So σ is surjective also. $\sigma \colon x \to x^p$ is isomorphism of $\mathbb{K}$ onto one of the subfield $\mathbb{K}^p$. Here map σ is called Frobenius map when $\sigma \colon \mathbb{F}_p \to \mathbb{F}_p$. □

Definition 7 (Field extension). *Let $\mathbb{K}$ and $\mathbb{F}$ be two fields. If $\mathbb{F} \subseteq \mathbb{K}$, then we call $\mathbb{K}$ is a field extension of $\mathbb{F}$ and we call $\mathbb{F}$ is a subfield of $\mathbb{K}$. We denote this by $\mathbb{K}/\mathbb{F}$.*

The field of real numbers $\mathbb{R}$ is extension of $\mathbb{Q}$, $\mathbb{C}$ is extension of $\mathbb{R}$. Every field is vector space over itself. If $\mathbb{K}$ is an extension field of $\mathbb{F}$ ($\mathbb{F} \subseteq \mathbb{K}$) then $\mathbb{K}$ is vector space over $\mathbb{F}$. If $\mathbb{K}$ is an extension field of $\mathbb{F}$ then degree of $\mathbb{K}$ over $\mathbb{F}$ is dimension of $\mathbb{K}$ as vector space over $\mathbb{F}$. We denote it by $f = [\mathbb{K} \colon \mathbb{F}]$ or simply $dim_{\mathbb{F}}\, \mathbb{K}$.

Definition 8 (Algebraic extension)**.** *A field extension $\mathbb{L}/\mathbb{K}$ is called algebraic extension if every element if $\mathbb{L}$ is algebraic over $\mathbb{K}$.*

Definition 9 (Algebraically closed field)**.** *A field $\mathbb{F}$ is called algebraically closed field if for every non-constant polynomial $f \in \mathbb{F}[X]$ has root in $\mathbb{F}$.*

Definition 10 (Algebraic closure)**.** *A field extension $\overline{\mathbb{F}}$ of $\mathbb{F}$ is called an algebraic closure if $\overline{\mathbb{F}}$ is an algebraic extension of $\mathbb{F}$ and $\overline{\mathbb{F}}$ is algebraically closed.*

An extension $\mathbb{F}$ of $\mathbb{K}$ is finitely generated if there are elements $r_1, r_2, \ldots, r_k$ in $\mathbb{F}$ such that $\mathbb{F} = \mathbb{K}(r_1, r_2, \ldots, r_k)$.

Definition 11 (Splitting fields)**.** *Let $\mathbb{K}$ be a field and $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ be a polynomial in $\mathbb{K}[X]$ of degree $n > 0$. An extension field $\mathbb{F}$ of $\mathbb{K}$ is called a splitting field for $f(x)$ over $\mathbb{K}$ if there exists elements $r_1, r_2, \ldots, r_n$ in $\mathbb{F}$ such that $f(x) = a_n(x - r_1)(x - r_2)\ldots(x - r_n)$ and $\mathbb{F} = \mathbb{K}(r_1, r_2, \ldots, r_n)$.*

Theorem 1.1.9.

1. *The characteristic of finite field $\mathbb{K}$ is prime number $p \neq 0$; if $f = [\mathbb{K} \colon \mathbb{F}_p]$, the number of elements of $\mathbb{K}$ is $q = p^f$.*

2. *Let p be prime number and let $q = p^f (f \geq 1)$ be a power of p. Let Ω be an algebraically closed field of characteristic p. There exists a unique subfield $\mathbb{F}_q$ of q elements. It is the set of roots of the polynomial $X^q - X$.*

3. *All finite field with $q = p^f$ elements are isomorphic to $\mathbb{F}_q$.*

Proof.

1. Here, $f = [\mathbb{K} \colon \mathbb{F}_p]$ as vector space. Then basis of $\mathbb{K}$ have f number of elements over $\mathbb{F}_p$. Let $\mathbb{K}$ has basis $B = \{b_1, b_2, \ldots, b_f\}$ over $\mathbb{F}_p$. Every element of $\mathbb{K}$ can be written as in the form of $\alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_f b_f$ where $\alpha_i \in \mathbb{F}_p$. $\#\mathbb{F}_p = p$, then each α_i have exactly p possibilities then there are p^f distinct linear combination of the form $\sum_{i=1}^{f} \alpha_i b_i$. Hence the number of elements in $\mathbb{K}$ is $q = p^f$.

2. The mapping $x \mapsto x^q$ is an isomorphism on Ω, because Ω is an algebraically closed field of characteristic p. The elements $\{x \in \Omega \mid x^q = x\}$ forms a subfield $\mathbb{F}_q$ of Ω. Derivative of given polynomial $X^q - X$ is
$$qX^{q-1} - 1 = p(p^{f-1}X^{q-1}) - 1 = -1,$$
which means the polynomial has q distinct roots. Now if $\mathbb{K}$ is subfield of Ω with q elements. Then $\mathbb{K}^*$ forms multiplicative group with $q - 1$ elements. Then for every element x of $\mathbb{K}^*$ satisfies $x^{q-1} = 1$ then $x^q = x$, because apart from $q - 1$ elements, zero is root of $X^q - X$ gives q roots of $X^q - X$.

3. Since $\mathbb{F}_q$ has q elements, we must have the factorization,

$$X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha).$$

It then follows from fact that both of the fields are splitting field of same polynomial $X^q - X$. For isomorphism, we refer the reader to [Hun73, Corollary 5.7 in page 280].

□

1.1.2 The multiplicative group of a finite field

Let p be prime number and $q = p^f$, where $f \geq 1$.

Theorem 1.1.10. *Let H be a group of order n. Then $H = \langle x^a \rangle$ if and only if $(a, n) = 1$. In particular the number of generators of H is $\varphi(n)$.*

Proof. Here $\langle x^a \rangle$ generates a subgroup of order $\#(x^a)$. This subgroup is equal to H if and only if $\#(x^a) = \#(x)$.

$$\#(x^a) = \#(x) \text{ if and only if } \frac{n}{(a, n)} = n,$$

i.e., if and only if $(a, n) = 1$. Since by definition of Euler's function $\varphi(n)$ is number of $a \in \{1, 2, 3, \ldots, n\}$ such that $(a, n) = 1$. □

In short, only those elements whose image in $\mathbb{Z}/n\mathbb{Z}$ is generator of this group. The number of generators of cyclic group of order d is $\varphi(n)$.

Proposition 1.1.11. *If H is a cyclic group of order n, then for each positive integer $a|n$, there is a unique cyclic subgroup $\langle x^{\frac{n}{a}} \rangle$ of H of order a.*

Proof. For a proof this proposition, refer to Thm 7 in [DF, p. 58]. □

Lemma 1.1.12. *If $n \geq 1$, then $n = \sum_{d|n} \varphi(d)$.*

Proof. For every d divides n, let C_d be the unique subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d and Φ_d be set of generators of C_d which gives by $\varphi(d)$, then all elements of $\mathbb{Z}/n\mathbb{Z}$ generate one of the C_d, the group $\mathbb{Z}/n\mathbb{Z}$ is the disjoint union of the Φ_d and

$$n = \#\mathbb{Z}/n\mathbb{Z} = \sum_{d|n} \#\Phi_d = \sum_{d|n} \varphi(d).$$

□

Lemma 1.1.13. *Let $\mathbb{F}_p^*$ be a finite group of order $p-1$. Suppose that for all divisors d of $p-1$, the set of $x \in \mathbb{F}_p^*$ such that $x^d = 1$ has at most d elements. Then $\mathbb{F}_p^*$ is cyclic.*

Proof. Let d be divisors of n. If there exists $x \in \mathbb{F}_p^*$ of order d, the subgroup $\langle x \rangle = \{1, x, x^2, \dots, x^{d-1}\}$ generated by x is cyclic of order d; in view of hypothesis, all elements $y \in \mathbb{F}_p^*$ such that $y^d = 1$ belong to $\langle x \rangle$. In particular, all elements of $\mathbb{F}_p^*$ of order d are generators of $\langle x \rangle$ and these are in number $\varphi(d)$. Hence, the number of elements of $\mathbb{F}_p^*$ of order d is either 0 or $\varphi(d)$. If it is zero for a value of d, the formula $\displaystyle\sum_{d|n}$ would show that the number of elements in $\mathbb{F}_p^*$ is $< n$, contrary to hypothesis. In particular, there exists an elements $x \in \mathbb{F}_p^*$ of order n and $\mathbb{F}_p^*$ coincides with the cyclic group $\langle x \rangle$. The equation $x^d = 1$, which has degree d, has at most d solutions in $\mathbb{F}_p^*$. □

1.2 Equations over a finite field

In this section, we will define the power sum and then we will use it to prove Chevalley-Warning theorem. Let $q = p^r$ for some $r \geq 1$, and let $\mathbb{K}$ be a field with q elements.

1.2.1 Power sums

Lemma 1.2.1. *Let $\mathbb{K}$ be a field with q elements. If f is a homomorphism of $\mathbb{K}$, and $y \in \mathbb{K}^*$ then $\sum_{x\in\mathbb{K}} f(x) = \sum_{x\in\mathbb{K}} f(x)f(y)$. Moreover, if $f(y) \neq 1$, then $\sum_{x\in\mathbb{K}} f(x) = 0$.*

Proof. Suppose $\mathbb{K} = \{x_1, x_2, \dots, x_q\}$. Since $\mathbb{K}$ is closed under multiplication by y, there is bijection between $\{x_1, x_2, \dots, x_q\}$ and $\{x_1y, x_2y, \dots, x_qy\}$. Since f is a homomorphism, we have

$$\sum_{x\in\mathbb{K}} f(x) = \sum_{x\in\mathbb{K}} f(x)f(y),$$

since every element x_i of $\mathbb{K}$ can be written as $x_i = x_jy$, for an unique j. Equivalently, the above equation is $(f(y)-1)\sum_{x\in\mathbb{K}} f(x) = 0$. So, if $f(y) \neq 1$, then $\sum_{x\in\mathbb{K}} f(x) = 0$. □

Lemma 1.2.2. *Let $\mathbb{K}$ be a field with $q = p^f$ elements. Then the sum*

$$S(X^u) = \sum_{x\in\mathbb{K}} x^u = \begin{cases} -1 & \text{if } u \geq 0 \text{ and } u \text{ is divisible by } q-1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If $u = 0$ and $x = 0$ then $x^u = 1$. If $u = 0$ then $\forall x \in \mathbb{K}$, $x^u = 1$ and $\#\mathbb{K} = q = p^f$

$$S(X^u) = \sum_{x\in\mathbb{K}} (x^u = 1) = \sum_{x\in\mathbb{K}} 1,$$

which implies that $S(X^u)$ is divisible by p and $\mathrm{Char}(\mathbb{K}) = p$ then $S(X^u) = q.1 = 0$. Now, if $u \geq 1$ and divisible by $q-1$, if $x = 0$ then $0^u = 0$ and if $x \neq 0$ then $u = (q-1)m$ for $m \in \mathbb{Z}$ and $S(X^u) = \sum_{x\in\mathbb{K}^*} x^{(q-1)m} = \sum_{x\in\mathbb{K}^*} 1$ (we show that $\mathbb{K}^*$ is cyclic group of order $q-1$ and $\mathrm{Char}(\mathbb{K}) = p$)

$$S(X^u) = \sum_{x\in\mathbb{K}^*} 1 = (q-1)\cdot 1 = -1.$$

If $q-1 \nmid u$, then $\exists\, y \in \mathbb{K}^*$ such that $y^u \neq 1$. By the lemma above, with $f(x) = x^u$ and $f(y) \neq 1$ we have $S(X^u) = 0$. □

1.2.2 Chevalley-Warning Theorem

Recall that $\mathbb{K}$ is a finite field with q elements, where $q = p^r$ for some $r \geq 1$.

Definition 12. *For $f \in \mathbb{K}[X_1, \dots, X_n]$, define*

$$S(f) = \sum_{(x_1,\dots,x_n)\in\mathbb{K}^n} f(x_1, \dots, x_n).$$

Lemma 1.2.3. *For any $f_i \in \mathbb{K}[X_i]$, we have*

$$S(f_1 f_2 \dots f_n) = S(f_1)S(f_2)\dots S(f_n). \tag{1.1}$$

Proof. We will prove it by induction. For $n = 1$, there is nothing to prove. Now for $n = 2$,

$$\begin{aligned} S(f_1f_2) &= \sum_{(x,y)\in\mathbb{K}^2} f_1(x)f_2(y) = \sum_{x\in\mathbb{K}}\sum_{y\in\mathbb{K}} f_1(x)f_2(y) \\ &= \left(\sum_{x\in\mathbb{K}} f_1(x)\right)\left(\sum_{y\in\mathbb{K}} f_2(y)\right) = S(f_1)S(f_2). \end{aligned}$$

Now, assume that (1.1) is true for $n = k$ and prove it for $n = k+1$.

$$S(f_1f_2\dots f_kf_{k+1}) = \sum_{(x_1,x_2,\dots,x_k,x_{k+1})\in\mathbb{K}^{n+1}} f_1(x_1)f_2(x_2)\dots f_{k+1}(x_{k+1})$$

$$= \sum_{x_1\in\mathbb{K}}\sum_{x_2\in\mathbb{K}}\dots\sum_{x_k\in\mathbb{K}}\sum_{x_{k+1}\in\mathbb{K}} f_1(x_1)f_2(x_2)\dots f_{k+1}(x_{k+1})$$

$$= \left(\sum_{x_1\in\mathbb{K}} f_1(x_1)\right)\left(\sum_{x_2\in\mathbb{K}} f_2(x_2)\right)\dots\left(\sum_{x_k\in\mathbb{K}} f_k(x_k)\right)\left(\sum_{x_{k+1}\in\mathbb{K}} f_{k+1}(x_{k+1})\right)$$

$$S(f_1f_2\dots f_kf_{k+1}) = S(f_1)S(f_2)\dots S(f_k)S(f_{k+1})$$

Hence it is true for $n \in \mathbb{N}$. □

Theorem 1.2.4 (Chevalley-Warning)**.** *Let $f_\alpha \in \mathbb{K}[X_1, X_2, \ldots, X_n]$ be polynomials in n variables such that $\sum_\alpha \deg f_\alpha < n$ and let V be the set of all common zeros in $\mathbb{K}^n$. Then $\#V \equiv 0 \pmod p$.*

Proof. Consider the polynomial $P = \prod_\alpha (1 - f_\alpha^{q-1})$ and $x_0 = (x_1, x_2, \ldots, x_n) \in \mathbb{K}^n$. If $x_0 \in V$, then $f_\alpha(x_0) = 0$ for all α, hence $P(x_0) = \prod_\alpha (1 - 0) = 1$. If $x_0 \notin V$ then $\exists\, \alpha$ such that $f_\alpha(x_0) \neq 0$. This implies that, $P(x_0) = 0$, because $\mathbb{K}^*$ is group of order $q - 1$ and $f_\alpha^{q-1}(x_0) = 1$. Hence,

$$P(x) = \begin{cases} 1 & \text{if } x \in V, \\ 0 & \text{if } x \notin V. \end{cases}$$

$$\begin{aligned} S(P) &= \sum_{(x_1,x_2,\ldots,x_n)\in\mathbb{K}^n} P(x_1, x_2, \ldots, x_n) \\ &= \sum_{(x_1,x_2,\ldots,x_n)\in V} P(x_1, x_2, \ldots, x_n) + \sum_{(x_1,x_2,\ldots,x_n)\notin V} P(x_1, x_2, \ldots, x_n) \end{aligned}$$

Since $P(x_1, x_2, \ldots, x_n) = 0$ if $(x_1, x_2, \ldots, x_n) \notin V$, then $\#S(P)$ is same as $\#V$. Now, it is enough to show that $S(P) = 0$. The polynomial P is linear combination of monomials $X_1^{u_1}, X_2^{u_2}, \ldots, X_n^{u_n}$ and $\sum_\alpha \deg f_\alpha < n$ then $\deg P < (q-1)n$ with $\sum u_i < (q-1)n$ and it is sufficient to prove that for at least one $u_i < q - 1$, since $\sum u_i < (q-1)n$ $\exists$ at least one u_i such that $u_i < q - 1$. Then by Lemma 1.2.2, it is clear that one of the $S(X^{u_i}) = 0$. Further by Lemma 1.2.3, its easy to see that

$$S(X_1^{u_1} X_2^{u_2} \ldots X_n^{u_n}) = S(X_1^{u_1}) S(X_2^{u_2}) \ldots S(X_n^{u_n}) = 0.$$

□

Corollary 1.2.5. *Let $f_\alpha \in \mathbb{K}[X_1, X_2, \ldots, X_n]$ be polynomials in n variables such that $\sum_\alpha \deg f_\alpha < n$ and if the f_α have no constant term, then the $\{f_\alpha\}_{\alpha\in\Lambda}$ have non-trivial common zeros.*

Proof. If V is $\{0\}$ then $\#V$ is not divisible by p. V has pm numbers of common zeros, where m is positive integer. Then we assure that f_α has $pm - 1$ non-trivial zeros. □

For example, one can see that all quadratic forms in at least three variables over $\mathbb{K}$ have a non-trivial zero. Let X, Y, Z be three variables in $\mathbb{K}$ and its quadratic form,

$$Q(X, Y, Z) = a_1X^2 + a_2Y^2 + a_3Z^2 + a_4XY + a_5YZ + a_6XZ = 0, \text{where } a_i \in \mathbb{K}.$$

Its clear that Q has trivial zero $(X, Y, Z) = (0, 0, 0)$. By Corollary 1.2.5, V has pm numbers of common zeros, where m is positive integer. Then we assure that Q have $pm - 1$ non-trivial zeros.

1.3 Quadratic reciprocity law

In number theory, the law of quadratic reciprocity has several hundred number of proofs. We will prove one of them, which is proved by Gauss. For that we need Legendre symbol, so first we will introduce Legendre symbol.

1.3.1 Squares in $\mathbb{F}_q$

Theorem 1.3.1. *Let q be a power of prime number p.*

1. *If $p = 2$, then all elements of $\mathbb{F}_q$ are squares.*

2. *If $p \neq 2$, then $(\mathbb{F}_q^*)^2$ forms a subgroup of index 2 on $\mathbb{F}_q^*$. In fact, the subgroup $(\mathbb{F}_q^*)^2$ is the kernel of the homomorphism $\sigma : x \to x^{\frac{(q-1)}{2}} \in \{\pm 1\}$, where $x \in \mathbb{F}_q^*$.*

Proof.

1. For $p = 2$, take map $\sigma : \mathbb{F}_q \to \mathbb{F}_q$, then its clear that $\sigma(x + y) = (x + y)^2 = x^2 + y^2 = \sigma(x) + \sigma(y)$ is homomorphism. Its easy to see that the kernel of this homomorphism is $\{0\}$, then we have invectiveness. Since, we have map σ form $\mathbb{F}_q$ to $\mathbb{F}_q$, its surjective also. Then, σ is automorphism. Hence, all elements of $\mathbb{F}_q$ are squares.

2. For $p \neq 2$, define map $\delta : \mathbb{F}_q^* \to \{\pm 1\}$ as $x \mapsto x^{\frac{(q-1)}{2}}$. If $x \in \mathbb{F}_q^*$ and $y \in \bar{\mathbb{F}}_q$ such that $y^2 = x$, then
$$y^{q-1} = x^{\frac{(q-1)}{2}} = \pm 1, \quad (\because x^{q-1} = 1).$$
For x to square in $\mathbb{F}_q$, it is necessary and sufficient that $y \in \mathbb{F}_q^*$, so that we have $y^(q - 1) = 1$ So $y \in \mathbb{F}_q^*$ i.e $y^{q-1} = 1$, and $\mathbb{F}_q^{*2}$ is kernel of $x \mapsto x^{\frac{(q-1)}{2}}$. Since $\mathbb{F}_q^*$ is cyclic group of order $q - 1$, index of $\mathbb{F}_q^{*2}$ is 2.

□

1.3.2 Legendre symbol

The classical methods only apply to quadratic equations over $\mathbb{C}$; efficiently solving quadratic equations over a finite field is a much harder problem. For a typical integer a and an odd prime p, its not even obvious a priori whether the congruence $x^2 \equiv a \pmod{p}$ has any solutions, much less what they are. By Fermats Little Theorem and some thought, it can be seen that a $a^{(p-1)/2} \equiv 1 \pmod{p}$ if and only if a is not a perfect square in the finite field. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$; otherwise, it is congruent to 1 (or 0, in the trivial case $a \equiv 0$). This provides a simple computational method of distinguishing squares from non squares in $\mathbb{F}_p$.

Definition 13. *Let p be odd prime and let $x \in \mathbb{F}_q^*$. Then the Legendre symbol of x is defined by $\left(\frac{x}{p}\right) = x^{(p-1)/2} = \pm 1 \in \mathbb{F}_q^*$, and if $a \in \mathbb{Z}$ and p be odd prime then $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$*

So congruent integers are of the same quadratic character. We can also define in terms of quadratic residue as follows :
$$\left(\frac{x}{p}\right) = x^{(p-1)/2} = \begin{cases} 0 & \text{if } x \text{ is a multiple of } p \text{ or } x = 0, \\ 1 & \text{if } x \text{ is a quadratic residue of } p, \\ -1 & \text{if } x \text{ is a quadratic non-residue of } p. \end{cases}$$

Definition 14. *An element $x \in \mathbb{Z}$ is said to be quadratic residue modulo p, if there exists an element $y \in \mathbb{Z}$ such that $y^2 \equiv x \pmod p$. Otherwise, the element x is said to be quadratic non-residue of p.*

Now, let us state some properties of the Legendre symbol.

1. If $x \in \mathbb{Z}$ and its image $x' \in \mathbb{F}_p$ then $\left(\frac{x}{p}\right) = \left(\frac{x'}{p}\right)$.
   Its clearly follows from quadratic character of congruent integers, because $x' \equiv x \pmod p$ then $y^2 \equiv x' \pmod p$ has a solution if and only if $x^2 \equiv x \pmod p$.

2. $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$.
   Follows directly from the identity $(ab)^{(p-1)/2} = a^{(p-1)/2}\, b^{(p-1)/2}$.

3. If $\left(\frac{x}{p}\right) = 1$ then $x \in \mathbb{F}_p^{*2}$.
   $\left(\frac{x}{p}\right) = x^{(p-1)/2} = 1 \Rightarrow x^{(p-1)/2} = 1 \quad$ then $x \in \mathbb{F}_p^{*2}$. $\quad$ ($\because$ order of $\mathbb{F}_p^{*2}$ is $(p-1)/2$).

4. If $x \in \mathbb{F}_p^*$ has y as a square root in $\overline{\mathbb{F}}_p^*$ then $\left(\frac{x}{p}\right) = y^{p-1}$.
   Easy to see that $\left(\frac{x}{p}\right) = x^{(p-1)/2} = y^{2((p-1)/2)} = y^{p-1}$.

Theorem 1.3.2. *For any odd prime p, the following formulas hold:*

1. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$,

2. $\left(\frac{-1}{p}\right) = (-1)^{(p^2-1)/8}$.

Proof. 1. If -1 is quadratic residue of p then it is 1, otherwise it is -1. Here note that if -1 is square $\pmod p$ then p can be written in the form $4k+1$ then it is 1, and -1 is not square $\pmod p$ then p is of the form then it is $4k-1$ then it is -1.

2. Let $\alpha \in \overline{\mathbb{F}}_p$ and it is 8^{th}-root of unity with $y = \alpha + \alpha^{-1} \in \overline{\mathbb{F}}_p$.
   then $y = \alpha + \alpha^{-1} \Rightarrow y^2 = \alpha^2 + 2 + \alpha^{-2}$, but α is $8^t h$ root of unity that is why $\alpha^4 = -1 and \alpha^2 + \alpha^{-1} = 0$. Hence, $y^2 = 2$. Now $y^p = \alpha^p + \alpha^{-p}$ and if prime p is $p \equiv \pm 1 \pmod 8$ then $y^p = \alpha + \alpha^{-1}$ which means $y^p = y \Rightarrow y^{p-1} = 1$ thus $\left(\frac{2}{p}\right) = 1$. and if p is $p \equiv \pm 5 \pmod 8$ then $y^p = \alpha^5 + \alpha^{-5}$ then
   $y^p = \alpha^4\alpha + \alpha^{-4}\alpha^{-1}(\because \alpha^4 = -1) \Rightarrow y^p = -(\alpha + \alpha^{-1}) = -y \Rightarrow y^{p-1} = -1$ thus $\left(\frac{2}{p}\right) = -1$.

□

1.3.3 Quadratic reciprocity law

Definition 15 (Gauss sum). *Let p and ℓ be two different odd prime numbers. Let $\mathbb{F}_p$, $\mathbb{F}_\ell$ be two fields and $w \in \overline{\mathbb{F}}_p$ with w be primitive ℓ^{th} root of unity. If $x \in \mathbb{F}_\ell$, then w^x is well defined because it is in one of the equivalence class of $\mathbb{F}_\ell$ and $w^x = 1$. Then the "Gauss sum" is defined by*

$$y = \sum_{x\in\mathbb{F}_\ell} \left(\frac{x}{\ell}\right) w^x.$$

From the above definition of y, it is not clear whether y is zero or not. The next lemma answers this question.

Lemma 1.3.3. *Let y be a Gauss sum defined as above, then one has $y^2 = (-1)^{(\ell-1)/2}\ell$.*

Proof. $y = \sum\limits_{x\in\mathbb{F}_\ell} \left(\frac{x}{\ell}\right) w^x$ and $y = \sum\limits_{z\in\mathbb{F}_\ell} \left(\frac{z}{\ell}\right) w^z$ then,

$$y^2 = \sum_{x\in\mathbb{F}_\ell} \left(\frac{x}{\ell}\right) w^x \sum_{z\in\mathbb{F}_\ell} \left(\frac{z}{\ell}\right) w^z.$$

$$y^2 = \sum_{x\in\mathbb{F}_\ell}\sum_{z\in\mathbb{F}_\ell} \left(\frac{x}{\ell}\right)\left(\frac{z}{\ell}\right) w^{x+z} = \sum_{x,z\in\mathbb{F}_\ell} \left(\frac{xz}{\ell}\right) w^{x+z}.$$

take $x + z = u$ and $x = t$ then $z = u - t$, $xz = t(u - t)$.

$$\sum_{x,z\in\mathbb{F}_\ell} \left(\frac{xz}{\ell}\right) w^{x+z} = \sum_{u\in\mathbb{F}_\ell} w^u \left(\sum_{t\in\mathbb{F}_\ell} \left(\frac{t(u-t)}{\ell}\right)\right).$$

Here we rearranging x, z in terms of t and u, because then whole sum convert in to just one variable u instead of x and z, and it is easy to calculate. Now if $t = 0$ then $y^2 = 0$ but we know that y can not be zero. Then if $t \neq 0$ then

$$\left(\tfrac{t(u-t)}{\ell}\right) = \left(\tfrac{(-t^2)(1-ut^{-1})}{\ell}\right) = \left(\tfrac{-t^2}{\ell}\right)\left(\tfrac{1-ut^{-1}}{\ell}\right) = (-1)^{(\ell-1)/2}\left(\tfrac{1-ut^{-1}}{\ell}\right)$$

and

$$(-1)^{(\ell-1)/2}y^2 = \sum_{u\in\mathbb{F}_\ell} C_u w^u,$$

where

$$C_u = \sum_{t\in\mathbb{F}_\ell^*} \left(\frac{1-ut^{-1}}{\ell}\right)$$

If $u = 0$ then $C_0 = \sum\limits_{t\in\mathbb{F}_\ell^*} \left(\frac{1}{\ell}\right) = \sum\limits_{t\in\mathbb{F}_\ell^*} 1 = \ell - 1$ For $u \neq 0$,$ut^{-1} = 1$ then $C_u = 0$ that means $s = 1 - ut^{-1}$ runs over $\mathbb{F}_\ell - \{1\}$, and then we have

$$C_u = \sum_{s\in\mathbb{F}_\ell}\left(\frac{s}{\ell}\right) - \left(\frac{1}{\ell}\right) = -\left(\frac{1}{\ell}\right) = -1.$$

In the above sum, $\sum\limits_{s\in\mathbb{F}_\ell^*}\left(\frac{s}{\ell}\right) = 0$, because of $\frac{\ell-1}{2}$ elements of $\mathbb{F}_\ell^*$ are squares (resp., non-squares) , hence the Legendre symbol is $+1$ (resp., -1). Hence,

$$\sum_{u\in\mathbb{F}_\ell^*} C_u w^u = -\sum_{u\in\mathbb{F}_\ell^*} w^u = +1 \Rightarrow \sum_{u\in\mathbb{F}_\ell^*} w^u = -1$$

because $w^\ell = 1 \Rightarrow w^\ell - 1 = 0$; $(w-1)(1+w+w^2+\ldots+w^{\ell-1}) = 0$
$\Rightarrow (1+w+w^2+\ldots+w^{\ell-1}) = 0 \quad (\because w \neq 1)$

$$\sum_{u\in\mathbb{F}_\ell} C_u w^u = \sum_{u=0} C_u w^u + \sum_{u\in\mathbb{F}_\ell^*} C_u w^u = \ell - 1 + 1 = \ell$$
$$y^2 = (-1)^{(\ell-1)/2}\ell.$$

□

The above lemma shows that the Gauss sum is non-zero, because of $(\ell, p) = 1$.

Lemma 1.3.4. *Let ℓ and p be two different primes and by Gauss sum $y^{p-1} = \left(\frac{p}{\ell}\right)$*

Proof. Since, $\mathrm{Char}(\overline{\mathbb{F}}_p) = p$, we have Gauss sum

$$y = \sum_{x\in\mathbb{F}_\ell}\left(\frac{x}{\ell}\right) w^x$$

then

$$y^p = \sum_{x\in\mathbb{F}_\ell}\left(\frac{x}{\ell}\right)^p (w^x)^p = \sum_{x\in\mathbb{F}_\ell}\left(\frac{x}{\ell}\right) w^x p$$

say $xp = z$,

$$\Rightarrow \sum_{x\in\mathbb{F}_\ell}\left(\frac{x}{\ell}\right) w^{xp} = \sum_{x\in\mathbb{F}_\ell}\left(\frac{zp^{-1}}{\ell}\right) w^z = \left(\sum_{z\in\mathbb{F}_\ell}\left(\frac{z}{\ell}\right) w^z\right)\left(\frac{p^{-1}}{\ell}\right) = \left(\frac{p}{\ell}\right) y;$$

$$\Rightarrow y^{p-1} = \left(\frac{p}{\ell}\right).$$

□

Theorem 1.3.5 (Quadratic reciprocity law by Gauss)**.**

$$\left(\frac{\ell}{p}\right) = (-1)^{\frac{\ell-1}{2}\frac{p-1}{2}}\left(\frac{p}{\ell}\right).$$

Proof.

$$y^2 = (-1)^{(\ell-1)/2}\ell$$

Both sides raise to the power $(p-1)/2$, then

$$y^{p-1} = (-1)^{\frac{(\ell-1)}{2}\frac{(p-1)}{2}}(\ell)^{(p-1)/2}$$

by previous result,

$$y^{p-1} = \left(\frac{p}{\ell}\right) = (-1)^{\frac{(\ell-1)}{2}\frac{(p-1)}{2}}(\ell)^{(p-1)/2} = (-1)^{\frac{(\ell-1)}{2}\frac{(p-1)}{2}}\left(\frac{\ell}{p}\right)$$

□

Chapter 2

p-adic fields

2.1 The ring $\mathbb{Z}_p$ and the field $\mathbb{Q}_p$

We will define p-adic integers $\mathbb{Z}_p$ by projective or inverse limit. We will see that p-adic integers forms ring and also subring of $\prod \mathbb{Z}/p^n\mathbb{Z}$. Exact sequence of $\mathbb{Z}_p$ will give some properties of p-adic integers and also gives relation with $\mathbb{Z}/p^n\mathbb{Z}$. Then we define topology on $\mathbb{Z}_p$. At the end of this section we will see p-adic numbers which is field of fraction of $\mathbb{Z}_p$.

2.1.1 Definitions

Let $p \in \mathbb{P}$. For any $n \geq 1$, $\mathbb{Z}/p^n\mathbb{Z}$ is ring of equivalence classes of integers modulo p^n. We will denote $A_n := \mathbb{Z}/p^n\mathbb{Z}$. Define the map $\varphi_n \colon \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$ such that

$$\varphi_n(x \pmod{p^n}) = (x \pmod{p^{n-1}}).$$

Then any element of $\mathbb{Z}/p^n\mathbb{Z}$ defines an element of $\mathbb{Z}/p^{n-1}\mathbb{Z}$.

Lemma 2.1.1. *Let map $\varphi_n : A_n \to A_{n-1}$ defined by $x \pmod{p^n} \to x \pmod{p^{n-1}}$ then for every $n \in \mathbb{N}$, the map φ_n is a homomorphism.*

Proof. If $\overline{x}_n, \overline{y}_n \in A_n$, then $\varphi_n(\overline{x}_n) = \overline{x}_{n-1}$, where $\overline{x}_{n-1} \in A_{n-1}$.

$$\varphi_n(\overline{x}_n + \overline{y}_n) = \varphi_n(\overline{x_n + y_n}) = \overline{x_{n-1} + y_{n-1}} = \overline{x}_{n-1} + \overline{y}_{n-1} = \varphi_n(\overline{x}_n) + \varphi_n(\overline{y}_n)$$

$$\varphi_n(\overline{x}_n\overline{y}_n) = \varphi_n(\overline{x_n y_n}) = \overline{x_{n-1}y_{n-1}} = \overline{x}_{n-1}\overline{y}_{n-1} = \varphi_n(\overline{x}_n)\varphi_n(\overline{y}_n)$$

Clearly, this map is surjective. because if $p^{n+1}\mathbb{Z} \subset p^n\mathbb{Z}$ then $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ is surjective. □

It is clear that, $\ker \varphi_n = \{\overline{x} \in A_n |\ \varphi_n(\overline{x}) = \overline{0}\} = p^{n-1}\mathbb{Z}/p^n\mathbb{Z}$

Definition 16 (Projective system). *Let X_i, X_j and X_k are non-empty sets and mapping $\varphi_{ij}\colon X_i \to X_j$ and $\varphi_{jk}\colon X_j \to X_k$ with $\varphi_{ik}\colon X_i \to X_k$ which is given by $\varphi_{ik} = (\varphi_{ij} \circ \varphi_{jk})$ which is true for any indexed by integer $i, j, k \geq 1$ then (X_{ij}, φ_{ij}) is called projective system.*

Definition 17 (Inverse/ Projective limit). *An inverse system is a sequence of objects (e.g. sets/groups/rings) (A_n) together with a sequence of morphisms (e.g. functions/homomorphisms) (f_n),*

$$\ldots A_i \xrightarrow{f_i} A_{i+1} \xrightarrow{f_{i+1}} A_{i+2} \xrightarrow{f_{i+2}} A_{i+3} \xrightarrow{f_{i+3}} \ldots$$

The inverse limit,

$$A = \varprojlim A_n$$

is the subset of the direct product $\prod_n A_n$ consisting of those sequences $a = (a_n)$ for which $f_n(a_{n+1}) = a_n$ for all $n \geq 1$. For each $n \geq 1$ the projection map $\pi_n : A \to A_n$ sends a to a_n.

We have $A_n = \mathbb{Z}/p^n\mathbb{Z}$ then for sequence,

$$\ldots A_{n+1} \to A_n \to A_{n-1} \ldots \to A_2 \to A_1$$

forms projective system with map $\varphi_n : A_n \to A_{n-1}$. An element of $\mathbb{Z}_p$ is sequence $(\ldots, x_n, \ldots, x_2, x_1)$ such that $x_n \in A_n$. We denote $(x_1, x_2, \ldots, x_n, \ldots)$ for element $(\ldots, x_n, \ldots, x_2, x_1)$. Addition and multiplication of elements of $\mathbb{Z}_p$ is component wise. So, $\mathbb{Z}_p$ forms ring.

The map that sends each integer $x \in \mathbb{Z}$ to the sequence $(\bar{x}, \bar{x}, \ldots, \bar{x}, \ldots)$ is a ring homomorphism, where $\bar{x}^{nth}$ is integer modulo p^n belongs to $\mathbb{Z}/p^n\mathbb{Z}$. Its kernel is clearly trivial, since 0 is the only integer congruent to 0 modulo p^n for all n. Thus the ring $\mathbb{Z}_p$ has characteristic 0 and contains $\mathbb{Z}$ as a subring, but $\mathbb{Z}_p$ is a much bigger ring than $\mathbb{Z}$. In subring of $\prod A_n$. We give A_n discrete topology and $\prod A_n$ product topology. Since each A_n is finite then it is compact and by Tychnoffs theorem $\prod A_n$ is also compact.

Theorem 2.1.2 (Tychnoff's theorem). *Arbitrary product of compact spaces is also compact.*

Lemma 2.1.3. *The ring $\mathbb{Z}_p$ is a compact space.*

Proof. To prove the lemma, it is enough that $\mathbb{Z}_p$ is a closed set in $\prod A_n$. For every $n \in \mathbb{N}$, define

$$B_n = \left\{ y \in \prod_{k=1}^{\infty} A_k \mid (\varphi_n \circ \pi_n \; - \; \pi_{n-1})(y) = \overline{0} \right\}$$

where $\pi_n\colon \mathbb{Z}_p \to A_n$ denotes the n-th projection. The map $(\varphi_n \circ \pi_n \; - \; \pi_{n-1})$ is a continuous map, hence B_n is closed being the inverse image of zero in A_n. Since, $\mathbb{Z}_p = \bigcap_{n=1}^{\infty} B_n$, hence $\mathbb{Z}_p$ is a closed subring of $\prod A_n$, which is a compact space by Tychnoff's theorem. Being a closed set of a compact space, $\mathbb{Z}_p$ is also compact. □

2.1.2 Properties of $\mathbb{Z}_p$

In this section we will talk about some useful relation between $\mathbb{Z}_p$ and A_n by exact sequence.

Definition 18. *(Exact sequence) : Consider functions f_i and non-empty sets A_i for which $f_i\colon A_i \to A_{i+1}$ forms homomorphisms then following sequence*

$$\cdots \quad A_i \xrightarrow{f_i} A_{i+1} \xrightarrow{f_{i+1}} A_{i+2} \xrightarrow{f_{i+2}} A_{i+3} \xrightarrow{f_{i+3}} A_{i+4} \quad \cdots$$

is said to exact sequence if $f_i(A_i) = \ker(f_{i+1})$ for all $i \geq 0$.

In our case we have short exact sequence of abelian group as follows.

$$A_0 = 0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \xrightarrow{f_3} A_3 \xrightarrow{f_4} 0 = A_4$$

Proposition 2.1.4. *The sequence $0 \to \mathbb{Z}_p \xrightarrow{f_n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} A_n \to 0$ is a short exact sequence of abelian groups. If $x \in \mathbb{Z}_p,\ f_n(x) = p^n x$ and $\varepsilon_n(x) = \overline{x}_n$ (n-th projection of x).*

Proof.

$$0 \xrightarrow{\eta_1} \mathbb{Z}_p \xrightarrow{f_n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} A_n \xrightarrow{\eta_2} 0$$

We prove this proposition with three steps as follows.
Step-I- f_n is injective.
Here sequence start from zero and we have homomorphisms. So, $\eta_1(0) = 0$. If we show $\ker f_n = \{0\}$ then we are done with our first step. Let $x \in \mathbb{Z}_p$ and $x \in \ker f_n$ then $p^n x = 0$ take $n = 1$ then $px = 0 \Rightarrow p\overline{x}_{n+1} = \overline{0}$ then $px_{n+1} \in p^{n+1}\mathbb{Z}$.

$$px_{n+1} \equiv 0 \pmod{p^{n+1}\mathbb{Z}}$$

i.e., $\exists\, \overline{y}_{n+1} \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ such that $px_{n+1} = p^{n+1}y_{n+1} \Rightarrow \overline{x}_{n+1} = p^n\overline{y}_{n+1}$, but according to our map,

$$\varphi_{n+1}(\overline{x}_{n+1}) = \varphi_{n+1}(p^n\overline{y}_{n+1}) = p^n\overline{y}_n = \overline{x}_n.$$

Then $\overline{x}_n$ is multiple of p^n, then it is 0. It is true for every n. So, $\ker f_n = \{0\} = \eta_1(0)$. Kernel of homomorphism is zero means map is injective, then for each n, $f_n\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is injective.
Step-II- $f_n(\mathbb{Z}_p) = \ker(\varepsilon_n)$.
For that we know $f_n(\mathbb{Z}_p) = p^n\mathbb{Z}_p$ and $\ker(\varepsilon_n) = \{x\colon \varepsilon_n(x) = 0\}$ for $x \in \mathbb{Z}_p$.
First we show $p^n\mathbb{Z}_p \subset \ker(\varepsilon_n)$. Let $x \in p^n\mathbb{Z}_p$, then $x = p^n y$ for $y \in \mathbb{Z}_p$,

$$\overline{x}_n = \varepsilon_n(x) = \varepsilon_n(p^n y) = p^n\varepsilon_n(y) = p^n\overline{y}_n = 0,$$

so $p^n\mathbb{Z}_p \subset \ker(\varepsilon_n)$. Now $\ker(\varepsilon_n) \subset p^n\mathbb{Z}_p$, $x \in \ker(\varepsilon_n)$ then $\varepsilon_n(x) = \overline{x}_n = 0$ i.e, $x_n \equiv 0 \pmod{p^n}$ and $x_m \equiv x_n \pmod{p^n}$ for $m \geq n$ then $x_m \equiv 0 \pmod{p^n}$,

$$x_m \equiv p^n y_{m-n} \pmod{p^m} \text{ for } y_{m-n} \in A_{m-n} \ (\because p^n\mathbb{Z}/p^m\mathbb{Z} \cong \mathbb{Z}/p^{m-n}\mathbb{Z}),$$

also,

$$x_m \equiv x_{m-1} \pmod{p^{m-1}} \text{ so} p^n y_{m-n} \equiv p^n y_{m-n-1} \pmod{p^{m-1}},$$

then $y_{m-n} \equiv y_{m-n-1} \pmod{p^{m-n-1}}$. i.e., two consecutive terms is congruent to modulo p^i and $\overline{x}_m = p^n\overline{y}_{m-n}$ then we have (sequence) element y by above congruent relation $p^n y = x$. As we have $y = (\overline{y}_1, \overline{y}_2, \ldots, \overline{y}_n, \ldots)$ and $x = (\overline{0}, \overline{0}, \ldots, \overline{0}(n^{th} term), \overline{x}_{n+1}, \ldots)$ but $p^n y = x$ and $x = p^n(\overline{y}_1, \overline{y}_2, \ldots, \overline{y}_n, \ldots) = (\overline{0}, \overline{0}, \ldots, \overline{0}(n^{th} term), p^n\overline{y}_{n+1}, \ldots)$ we have to show that $y_{n+1} \equiv y_1 \pmod{p}$.

$$\begin{aligned} y_{n+1} &\equiv y_n \pmod{p^n} \\ y_n &\equiv y_{n-1} \pmod{p^{n-1}} \\ &: \quad : \\ y_3 &\equiv y_2 \pmod{p^2} \\ y_2 &\equiv y_1 \pmod{p} \end{aligned}$$

So, $y_{n+1} \equiv y_1 \pmod{p}$.

Step-III- ε_n is surjective.

By taking $\overline{y}_n \in \mathbb{Z}/n\mathbb{Z}$, and since we have inverse limit gets an element $y \in \mathbb{Z}_p$, by $\varprojlim A_n = \mathbb{Z}_p$ as an element $x = p^n y$. So ε_n is surjective. □

Proposition 2.1.5. *For an element of $\mathbb{Z}_p$ (resp., of A_n) to be invertible if and only if it is not divisible by p.*

Proof. To show that $x \in \mathbb{Z}_p$ is invertible if and only if it is not divisible by p, case of A_n will follow for $\mathbb{Z}_p$ invertible. Suppose $\overline{x}_1 \in A_1$ is invertible then $\overline{x}_1 \in A_1$ is not multiple of p. Now $\overline{x}_2 \neq 0$, because if $\overline{x}_2 = 0$ then by surjective map $\varphi(A_2) = A_1$, $\overline{x}_1 = 0$ but $\overline{x}_1 \neq 0$ so $\overline{x}_2 \neq 0$. Hence not multiple of p^2 and so on. Thus $x \in \mathbb{Z}_p$ is invertible then it is not divisible by p. Conversely, $x \in \mathbb{Z}_p$ is not divisible by p. $x \neq py$ for $y \in \mathbb{Z}_p$, but it is sufficient to show that any $\overline{x}_n \in A_n$ is not divisible by p then we are done. i.e., $\overline{x}_n \in A_n$ but $\overline{x}_n \notin pA_n$ then $\overline{x}_1 \notin pA_1 \Rightarrow \overline{x}_1 \neq 0$ thus $\overline{x}_1$ is invertible then $\overline{x}_n$ is invertible. That means $\exists\, \overline{y}_n \in A_n$ such that $\overline{x}_n\overline{y}_n = \overline{1}(p^n)$ so that $x_n y_n - 1 \in p^n\mathbb{Z} \Rightarrow x_n y_n - 1 = p^n a_n$ for $a_n \in \mathbb{Z}$. Take $p^{n-1}a_n = z_n$ then $x_n y_n = 1 + p^n a_n \Rightarrow x_n y_n = (1 - p^n a_n) \Rightarrow x_n y_n(1 - pz_n) \Rightarrow x_n y_n(1 + pz_n + p^2 z_n^2 + \ldots) = 1$, because $\overline{x}_n\overline{y}_n = \overline{1}$. Applying φ we get $\varphi_n(\overline{x}_n) = \overline{x}_{n-1}$ but

$\varphi_n(\overline{x}_n\overline{y}_n) = \varphi_n(\overline{x}_n)\varphi_n(\overline{y}_n) = \overline{1} \Rightarrow \overline{x}_{n-1}\varphi_n(\overline{y}_n) = 1$ then $\varphi_n(\overline{y}_n) = (\overline{x}_{n-1})^{-1}$. i.e. $\exists\, \overline{y}_{n-1} \in A_{n-1}$, which forces to be inverse of $\overline{x}_{n-1}$. Thus x is invertible. □

Let U denote the group of all invertible elements of $\mathbb{Z}_p$, we call them as p-adic units.

Proposition 2.1.6. *Every non-zero element of $\mathbb{Z}_p$ can be written uniquely in the form $p^n u$ with $u \in U$ and $n \geq 0$.*

Proof. Take $x \neq 0$ then $\exists$ a largest positive integer $n \geq 0$ such that $\overline{x}_n = \varphi_n(x)$ is zero, so $x = p^n u$ and u is not divisible by p, because if u is divisible by p then $x = p^{n+1}u_1$ and $\overline{x}_{n+1} = \overline{0}$. Since its contradict to our largest integer n, u is not divisible by p, thus it is invertible and then $u \in U$.
Uniqueness - Let $x_1 = p^n u_1$ and $x_1 = p^m u_2$ for $m \neq n$ and $u_1 \neq u_2$ then $p^n u_1 = p^m u_2$, (WLOG $m \geq n$) then $u_1 = p^{m-n}u_2$ but u_1 is invertible so it is not divisible by p. So $m = n$. Since, $m = n$ we can cancel it, and then we have $u_1 = u_2$, which means injective. We conclude that non-zero element of $\mathbb{Z}_p$ can be written uniquely $p^n u, \; u \in U$. □

By above proposition, we have that every non-zero element $x \in \mathbb{Z}_p$ can be written uniquely as
$x = p^n u$,

Definition 19 (p-adic valuation)**.** *Define the p- adic valuation of x to be n, which we denote by $\nu_p(x) = n$. If $x = 0$, then we define $\nu_p(0) = \infty$.*

Next two proposition gives properties of valuation p-adic integers.

Proposition 2.1.7. *$x = p^n u_1$, $y = p^m u_2$ be two p-adic integers then $\nu_p(xy) = \nu_p(x) + \nu_p(y)$.*

Proof. $xy = p^{m+n}u_1u_2$. So by definition of p-adic valuation
$\nu_p(xy) = \nu_p(p^{m+n}u_1u_2) = n + m = \nu_p(x) + \nu_p(y)$. □

Proposition 2.1.8. $\nu_p(x+y) \geq \inf\{\nu_p(x), \nu_p(y)\}$ *for two p-adic integers x and y.*

Proof. Let $x = p^n u_1, y = p^m u_2$ and WLOG $m \geq n$ then $x + y = p^n(u_1 + p^{m-n}u_2)$. p-adic valuation of $x + y$, $\nu_p(x+y) = \nu_p(p^n(u_1 + p^{m-n}u_2)) \geq n = \inf\{\nu_p(x), \nu_p(y)\}$. □

Lemma 2.1.9. *$\mathbb{Z}_p$ is PID. (Ideals of ring $\mathbb{Z}_p$ is $p^n\mathbb{Z}_p$).*

Proof. Let I be a non-zero ideal of $\mathbb{Z}_p$. By well-ordering principle take $a(\neq 0) \in I$ such that a have minimal valuation in I, say $\nu_p(a) = k > 0$. Then $a = p^k u$,$u \in \mathbb{Z}_p^\times$. So $a\mathbb{Z}_p = p^k\mathbb{Z}_p \subset I$. Now, $I \subset p^k\mathbb{Z}_p$, If $I \not\subset p^k\mathbb{Z}_p$ then $\exists\, b \in I$ but $b \notin p^k\mathbb{Z}_p$ but then b must have smaller valuation than k, which contradict to minimality of k. □

Proposition 2.1.10. *The distance* $d(x,y) = e^{\nu_p(x-y)}$ *satisfies something more than triangle inequality which is "ultrametric" inequality,*

$$d(x,z) \leq \sup\{d(x,y), d(y,z)\} \leq d(x,y) + d(y,z).$$

Proof. Start with triangle inequality $d(x,z) \leq d(x,z) + d(y,z)$, We can write $x - z = (x-y) + (y-z)$. By taking valuation,

$$\begin{aligned} \nu_p(x-z) &= \nu_p(x-y) + \nu_p(y-z) \\ &\geq \inf\{\nu_p(x-y), \nu_p(y-z)\} \\ &\geq \inf\{\nu_p(x-y), \nu_p(y-z)\} \\ \Rightarrow -\nu_p(x-z) &\leq -\inf\{\nu_p(x-y), \nu_p(y-z)\} \\ \Rightarrow -\nu_p(x-z) &\leq \sup\{-\nu_p(x-y), -\nu_p(y-z)\}, \end{aligned}$$

by taking exponential both side we get,

$$e^{-\nu_p(x-z)} \leq \sup\{e^{-\nu_p(x-y)}, e^{-\nu_p(y-z)}\} \Rightarrow d(x,z) \leq \sup\{d(x,y), d(y,z)\}.$$

Its, obvious that $d(x,z) \leq \sup\{d(x,y), d(y,z)\} \leq d(x,y) + d(y,z)$. □

Proposition 2.1.11. *p-adic integers is metric space with distance* $d(x,y) = e^{-\nu_p(x-y)}$.

Proof. Let $x, y \in \mathbb{Z}_p$, then we have distance $d(x,y) = e^{-\nu_p(x-y)}$.

1. if $x = y \iff d(x,y) = e^{-\nu_p(0)} \iff d(x,y) = 0 \quad (\because \nu_p(0) = \infty)$
2. $d(x,y) = e^{-\nu_p(x-y)} = e^{-\nu_p(y-x)} = d(y,x)$.
3. $d(x,y) \leq d(x,z) + d(z,y)$.
   Triangle inequality clear from Proposition 2.1.10. Hence, d defines metric.

□

Proposition 2.1.12. *The topology on $\mathbb{Z}_p$ is defined by distance $d(x,y) = e^{-\nu_p(x-y)}$. The ring $\mathbb{Z}_p$ is complete metric space and $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.*

Proof. $\mathbb{Z}_p$ is metric space. So take N be neighborhood of zero, $0 \in N$ then $\exists\, \epsilon > 0$ such that $0 \in B(0,\epsilon) \subseteq N$. Now take radius to be e^{-p^n} then $B(0, e^{-p^n}) = \{x \colon d(0,x) < e^{-p^n}\} = \{x \colon e^{-\nu_p(x)} < e^{-p^n}\} \Rightarrow \nu_p(x) > p^n$. It is clear that $B(0, e^{-p^n}) = p^{n+1}\mathbb{Z}_p$ $(\because p^{n+2}\mathbb{Z}_p \subset p^{n+1}\mathbb{Z}_p)$. We know that compact implies complete and totally bounded and we have already product topology which is compact. For denseness, let z_n be an arbitrary sequence in $\mathbb{Z}$. If $x = (x_n)$ is an element of $\mathbb{Z}_p$ such that $z_n \equiv x_n \pmod{p^n}$ then $\lim z_n = x$, which proves that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.

□

2.1.3 The field $\mathbb{Q}_p$

Definition 20. *The field of fractions of the ring $\mathbb{Z}_p$ is field of p-adic numbers which is $\mathbb{Q}_p$.*

Every non-zero element of $\mathbb{Q}_p$ can be written uniquely in the form of $p^n u$ where u is unit element of $\mathbb{Q}_p$. Valuation of elements of $\mathbb{Q}_p$ is same as elements of $\mathbb{Z}_p$ but only thing to notice that is in $\mathbb{Z}_p$ valuation is from $\mathbb{N} \cup \{\infty\}$, wheres in $\mathbb{Q}_p$ it is from $\mathbb{Z} \cup \{\infty\}$. Note that valuation of an element is ≥ 0 if and only if that element is in $\mathbb{Z}_p$.

Proposition 2.1.13. *The topology defined on the field $\mathbb{Q}_p$ with same distance $d(x, y) = e^{-\nu_p(x-y)}$ is locally compact. Since, $\mathbb{Z}_p$ is an open subring of $\mathbb{Q}_p$, also field $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.*

Proof. Since, $\mathbb{Z}_p$ is compact subspace of $\mathbb{Q}_p$ and close unit ball in $\mathbb{Q}_p$. Let x be an element of $\mathbb{Q}_p$, then $x + \mathbb{Z}_p$ is compact neighborhood of x. That means we have compact neighborhood for any arbitrary element. Hence, $\mathbb{Q}_p$ is locally compact, by neighborhood of zero and subspace of $\mathbb{Q}_p$. □

Proposition 2.1.14. *A sequence $x_n \in \mathbb{Z}_p$ has limit if and only if $\lim(u_{n+1} - u_n) = 0$.*

Proof. Suppose x_n has limit ℓ, i.e., for every $\epsilon > 0 \ \exists \ N > 0$ such that $n \geq N$ then $d(x_n, \ell) < \epsilon$. Say $a_n = (x_{n+1} - x_n)$ then

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} x_{n+1} - \lim_{n\to\infty} x_n = \ell - \ell = 0.$$

Now if $\lim\limits_{x\to\infty}(x_{n+1} - x_n) = 0$ i.e., $\forall \ \epsilon > 0 \ \exists \ N \geq 0$ such that $n \geq N, \ x_{n-1} - x_n < \epsilon$. Here $\mathbb{Z}_p$ is complete, so its remain to show that it is Cauchy, $\forall m, n \geq N$.

$$d(x_m, x_n) \leq \sup\{d(x_m, x_{m-1}), d(x_{m-1}, x_{m-2}), \ldots, d(x_{n-1}, x_n)\} < \epsilon.$$

Hence, we are done. □

Proposition 2.1.15. *A series in $\mathbb{Z}_p$ is converges if and only if its general term tends to zero.*

Proof. A Series is convergent if and only if the sequence of partial sums is convergent, i.e., $\sum a_n$ is convergent to s, if $S_n = \sum_{k=1}^{n} a_k$ converges to s. Suppose if series is convergent then $a_n = S_n - S_{n-1} \to 0$ as $n \to \infty$.

$$\lim_{n\to\infty} S_{n+1} - S_n = 0$$

Its similar case of sequence, here we have sequence of partial sum, and its Cauchy. Since, $\mathbb{Z}_p$ is complete space, it has limit. Then we have limit of sequence. □

2.2 p-adic equations

In this section we will see equivalent relation of zeros between p-adic numbers, p-adic integers and A_n. Then prove one important result Hensel's lemma in single variable, prove in several variable also.

2.2.1 Solutions

Lemma 2.2.1. *Let $\ldots \to D_n \to D_{n-1} \to \ldots \to D_2 \to D_1$ be a projective system, and let $D = \varprojlim D_n$ be its projective limit. If the D_n are finite and nonempty, then D is nonempty.*

Proof. case-1) If map $\varphi : D_n \to D_{n-1}$ is surjective, $D'_n s(\forall n)$ are nonempty and finite then D is non-empty. Let $x_1 \in D_1$, and map is surjective so that we can find its inverse image in D_2 and so on. From this we get $D = \varprojlim D_n$. Or for any $n > 1$ look at D_n and we have surjective map, So this map allows us to reach up to D_1. By taking inverse limit $D = \varprojlim D_n$.
case-2) If $\varphi : D_n \to D_{n-1}$ is not surjective, and $D'_n s(\forall n)$ are nonempty and finite.
To prove this, denote $D_{n,p}$ is image of D_p in D_n.(For ex. $\varphi(D_4)$ in D_2 is $D_{2,4}$ and $\varphi(D_2)$ in D_1 is $D_{1,2}$). Note that here p is not prime number but $p \in \mathbb{N}$. It is clear that $D_{n,p}$ forms decreasing family of finite nonempty subsets, also $D'_n s(\forall n)$ are finite, so family of subsets is stationary. Let say for large p, $D_{n,p}$ is stationary.(i.e. There is no effect of φ after stationary point p and then $D_{n,p} = D_{n,m}$, where $\forall\ m \geq p$). Denote this stationary level by E_n ($\forall\ n$). Now we want to show that the map $\varphi : E_n \to E_{n-1}$ is surjective and we will prove inductively. First we see for $\varphi : E_2 \to E_1$. Let $E_1 \subseteq D_1$ is stationary for D_1. For this take any element $x_1 \in D_{1,p} = E_1$ for p large enough. Then it has inverse image in D_2, because it is stationary so its allows us to take same element in $D_{1,m}$ where $\forall m > p$ and by taking inverse image in that D_2. D_2 have also stationary level E_2, by that we can see that $\varphi : E_2 \to E_1$ is surjective. By doing same process for n, $D_n \to D_{n-1}$ carries E_n onto E_{n-1}. Hence by taking inverse limit of $E'_n s$ we get $\varprojlim E_n = E \neq \emptyset$ so that $\varprojlim D_n = D$. □

If $f \in \mathbb{Z}_p[X_1, x_2, \ldots, X_m]$ is polynomial with coefficients in $\mathbb{Z}_p$ and $n \geq 1$ then f_n is polynomial with coefficients in A_n getting from taking reduction modulo p^n of polynomial f, but by exact sequence we know that $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong A_n$ So, reduction modulo p^n is in A_n.

Lemma 2.2.2. *Let $\{f_i\}_{i\in\Lambda} \in \mathbb{Z}_p[X_1, X_2, \ldots, X_m]$ be polynomial with p-adic integer coefficients then following are equivalent, where Λ is indexing set.*

1. *The polynomials $\{f_i\}_{i\in\Lambda}$ have a common zero in $(\mathbb{Z}_p)^m$.*

2. *The polynomials $\{(f_i)_n\}_{i\in\Lambda}$ have a common zero in $(A_n)^m$, for all $n > 1$.*

Proof. If we can show that $D = \varprojlim D_n$ then we are done, where D is set of all common zero of $\{f_i\}$, and D_n be set of all common zero of polynomials $\{(f_i)_n\}_{i\in\Lambda}$. We denote polynomials $\{f_{(i,n)}\}_{i\in\Lambda}$ for $\{(f_i)_n\}_{i\in\Lambda}$. Let D be a set of all common zero of $\{f_i\}_{i\in\Lambda}$ in $(\mathbb{Z}_p)^m$. Take projection on any $n > 1$, i.e., by taking reduction modulo p^n we have common zero D_n of polynomials $\{f_{(i,n)}\}_{i\in\Lambda}$ in $(A_n)^m$, for all $n > 1$, where D_n is set of all common zero of polynomials $\{f_{(i,n)}\}_{i\in\Lambda}$ in $(A_n)^m$, for all $n > 1$. Any zero of $f_{(i,n)}$ by taking modulo p^n is in D_n, also taking modulo p of zero of $f_{(i,n)}$ will be zero of $f_{(i,n+1)}$ in D_{n+1} i.e., taking modulo p of zero of $f_{(i,n)}$ will be in D_{n+1} is same as taking modulo p^{n+1} of zero of $\{f_i\}$ will be in D_{n+1} and also both zeros are same, then we have map from D_{n+1} to D_n. Then by Lemma 2.2.1 we have $D \subseteq \varprojlim D_n$. Let D_n be set of all common zero of polynomials $f_{i,n}$, for all $n > 1$. Suppose $z_n = ((z_{n,1}, z_{n,2}, \dots, z_{n,m})$ be common zero in D_n, also $z_n \in (A_n)^m$. For $n = 1$, $z_1 = (z_{1,1}, z_{1,2}, \dots, z_{1,m})$ then
$f_{(i,1)}(z_1, z_2, \dots, z_m) = 0 = (0_1, 0_2, \dots, 0_m) \in (A_1)^m \;\Rightarrow\; f_{(i,1)}(z_1, z_2, \dots, z_m)$ is common zero in $(A_1)^m$ which means multiple of p. Then if we take z to be common zero of $\{f_i\}$ as

$$z = ((z_{1,1}, z_{2,1}, \dots), (z_{2,1}, z_{2,2}, \dots), \dots, (z_{1,m}, z_{2,m}, \dots)) \in (\mathbb{Z}_p)^m$$

Then $f_i(x) = 0 \Rightarrow \varprojlim D_n \subseteq D$. Hence we have $\varprojlim D_n = D$. □

Definition 21 (Primitive zero). *A point $x = (x_1, x_2, \dots, x_m) \in (\mathbb{Z}_p)^m$ is called a primitive solution, if one of the x_i is invertible, i.e., x_i not divisible by p. A similar notion can be defined for primitive elements of $(A_n)^m$.*

Lemma 2.2.3. *Let $\{f_i\}_{i\in\Lambda} \in \mathbb{Z}_p[X_1, X_2, \dots, X_m]$ be a set of homogeneous polynomials with coefficients in $\mathbb{Z}_p$, then following are equivalent.*

1. *The polynomials $\{f_i\}_{i\in\Lambda}$ have a non-trivial common zero in $(\mathbb{Q}_p)^m$.*

2. *The polynomials $\{f_i\}_{i\in\Lambda}$ have a common primitive zero in $(\mathbb{Z}_p)^m$.*

3. *The polynomials $\{f_{(i,n)}\}_{i\in\Lambda}$ have common primitive zero in $(A_n)^m$, for all $n > 1$.*

Proof. $1 \;\Rightarrow\; 2)$ Let $x = (x_1, x_2, \dots, x_m)$ is non-trivial common zero of $\{f_i\}$ in $(\mathbb{Q}_p)^m$, then take infimum of all valuations of $x_i's$. Say $h = \inf\{\nu_p(x_1), \nu_p(x_2), \dots, \nu_p(x_m)\}$ then look at new element y as $y = p^{-h}x$. Then y is primitive element and we have homogeneous polynomial so that

$$f(y) = f(p^{-h}x_1, p^{-h}x_2, \dots, p^{-h}x_m) = p^{\alpha} f(x_1, x_2, \dots, x_m) = 0$$

where $\alpha \in \mathbb{N}$. Conclude that y is common primitive zero of $\{f_i\}$ in $(\mathbb{Z}_p)^m$.
$2 \;\Rightarrow\; 1)$ Suppose $\{f_i\}$ have common primitive zero in $(\mathbb{Z}_p)^m$. Let $x = (x_1, x_2, \dots, x_m)$ is common primitive zero of $\{f_i\}$ in $(\mathbb{Z}_p)^m$, then one of the x_i is invertible, which means it is not multiple of p.

Hence it is non-zero. Then same x is non-trivial common zero. Then $\{f_i\}$ have non-trivial common zero in $(\mathbb{Q}_p)^m$.
$2 \Rightarrow 3)$ Let y be common primitive zero of $\{f_i\}$ in $(\mathbb{Z}_p)^m$. Then one of the y_i is invertible from $y = (y_1, y_2, \ldots, y_m)$ which implies that particular y_i is not multiple of p. Take

$$y_n = (y_1 \pmod{p^n}, y_2 \pmod{p^n}, \ldots, y_m \pmod{p^n})$$

is reduction modulo of y by p^n for all $n > 0$. Then image of same y_i with modulo p^n is also invertible. Hence $y_n = (y_1 \pmod{p^n}, y_2 \pmod{p^n}, \ldots, y_m \pmod{p^n})$ is $\{f_{(i,n)}\}$ is common primitive zero in $(A_n)^m$, for all $n > 0$.
$3 \Rightarrow 2)$ Let $x_n \in (A_n)$ be common primitive zero of $\{f_{(i,n)}\}$. For $n = 1, x_1 = (x_{1,1}, x_{1,2}, \ldots, x_{1,m})$ is common primitive zero of $\{f_{(i,1)}\}$, then one of the $x_{(1,j)}$ where $1 \leq j \leq m$ is invertible in $(A_1)^m$. This implies that $x_{(1,j)}$ is not multiple of p. We can get $x_2 \in (A_2)^m$ by taking modulo p of x_1, one can do for any x_n by taking modulo p^{n-1}. Then look at the new element

$$x = ((x_{1,1}, x_{2,1}, \ldots), (x_{2,1}, x_{2,2}, \ldots), \ldots, (x_{1,m}, x_{2,m}, \ldots)) \in (\mathbb{Z}_p)^m$$

Hence it is common primitive zero of $\{f_i\}$, because image of $x_{(1,j)}$ in any A_n is invertible. □

2.2.2 Approximate solutions

We are concerned in passing from a solution $\pmod{p^n}$ to a solution in $\mathbb{Z}_p$.

Lemma 2.2.4 (Hensel's lemma)**.** *Let f be a polynomial in $\mathbb{Z}_p[X]$ and f' be its derivative. Let $x \in \mathbb{Z}_p$ and $n, k \in \mathbb{Z}$ such that $0 \leq 2k < n, f(x) \equiv 0 \pmod{p^n}, \nu(f'(x)) = k$. Then there exists $y \in \mathbb{Z}_p$ such that $f(y) \equiv 0 \pmod{p^{n+1}}, \nu(f'(x)) = k$ and $y \equiv x \pmod{p^{n-k}}$.*

Proof. Let $f(x) = p^n b$ and $f'(x) = p^k c$ where $b = p^i u_1 \in \mathbb{Z}_p, c \in U$. Take $z \in \mathbb{Z}_p$ then $z = p^j u_2$.

$$b + zc = p^i u_1 + p^j u_2 c = p^i (u_1 + p^{j-i} u_2 c)$$

$b + zc \equiv 0 \pmod{p} \Rightarrow \exists\, z$ such that we can choose $b + zc \equiv 0 \pmod{p}$ and then $z \equiv -bc^{-1} \pmod{p}$. By applying Taylor's formula with $y = x - p^{n-k} bc$,

$$\begin{aligned} f(y) &= f(x) + p^{n-k} f'(x) + p^{2n-2k} f''(x) + \ldots \\ &= p^n b - p^{n-k} bcp^k c + p^{2n-2k}(-bc)^2 f''(x) + \ldots \\ &= p^n b - p^n bc^2 + p^{2n-2k}(-bc)^2 f''(x) + \ldots \\ \Rightarrow f(y) &\equiv 0 \pmod{p^{n+1}} \qquad (\because 2n - 2k > n \text{ and } b + zc \equiv 0 \pmod{p}) \end{aligned}$$

Now applying Taylor's formula on $f^{'}(x)$,

$$\begin{aligned} f'(y) &= f'(x) - p^{n-k}bcf''(x) + \dots \\ &= p^k c - p^{n-k}bcf^{''}(x) + \dots \\ f'(y) &\equiv p^k c \pmod{p^{n-k}}, \end{aligned}$$

but we have to see that in $f'(y) = p^k c + p^{n-k}x$, where $x \in \mathbb{Z}_p$, $c + p^{n-k}x$ is also unit element in $\mathbb{Z}_p$. If $c + p^{n-k}x$ is not unit than $p|c + p^{n-k}x$, which implies p divides both c and $p^{n-k}x$, but here c is unit element, which says that $c + p^{n-k}x$ is unit element in $\mathbb{Z}_p$. Hence we are done. □

Now, we see the Hensel's lemma in several variable.

Theorem 2.2.5. *Let $f \in \mathbb{Z}_p[X_1, X_2, \dots, X_m]$, $x \in (\mathbb{Z}_p)^m$, $n, k \in \mathbb{Z}$ and j be an integer such that $0 < j \leq m$. Suppose that $0 \leq 2k < n$ and that $f(x) \equiv 0 \pmod{p^n}$ and $\nu_p\left(\frac{\partial f}{\partial X_j}(x)\right) = k$. Then there exists zero y of f in $(\mathbb{Z}_p)^m$ with $y \equiv x \pmod{p^{n-k}}$.*

Proof. First we will prove theorem for $m = 1$, then we generalize in m variables. Let take m to be 1, then by applying Lemma 2.2.4 to $x_0 = x$. We get $x_1 \in \mathbb{Z}_p$ which is also satisfies $x_1 \equiv x_0 \pmod{p^{n-k}}$ such that

$$f(x_1) \equiv 0 \pmod{p^{n+1}} \quad \text{and} \quad \nu_p(f'(x_1)) = k.$$

Now if we apply same lemma on x_1, then we get x_2. By arguing inductively we can construct sequence $x_0, x_1, x_2, \dots, x_t, \dots$ such that

$$x_{t+1} \equiv x_t \pmod{p^{n+t-k}} \quad \text{and} \quad f(x_t) \equiv 0 \pmod{p^{n+t}}$$

Then $\nu_p(x_{t+1} - x_t)$ is $n + t - k$ but it is goes to infinity as $t \to \infty$ and zero is the only element whose valuation is infinity. Then we have Cauchy sequence. Suppose y is limit, i.e.,

$$\lim_{t \to \infty} \left(f(x_t) \equiv 0 \pmod{p^{n+t}}\right)$$

as $n + t \to \infty$ we have $f(y) = 0$ and $y \equiv x \pmod{p^{n-k}}$, hence the theorem for $m = 1$. Now we will see theorem for m variables. Here this case is also reduces to $m = 1$. First we have given zero $x = (x_1, x_2, \dots, x_m)$. If we replacing X_i for all $i \neq j$ by x_i then the same polynomial $\tilde{f} \in \mathbb{Z}_p[X_j]$ be polynomial in one variable. Now we can apply Lemma 2.2.4 on $\tilde{f}$. Then we get $y_j \equiv x_j \pmod{p^{n-k}}$ such that $\tilde{f}(y_j) = 0$ by substituting $y_i = x_i$ for all $i \neq j$, then $y = (x_1, x_2, \dots, y_j, \dots, x_m) = (y_1, y_2, \dots, y_j, \dots, y_m)$ will satisfies $y \equiv x \pmod{p^{n-k}}$ and $f(y) = 0$. □

Definition 22 (Simple zero)**.** *If f is polynomial in $m > 1$ variables over field $\mathbb{F}$, then a zero x of f is said to be simple if at least one of the partial derivatives $\frac{\partial f}{\partial X_j}(x) \neq 0$.*

Corollary 2.2.6. *Every simple zero of the reduction modulo p of a polynomial f lifts to a zero of f in $\mathbb{Z}_p$.*

Proof. This is special case of Theorem 2.2.5 when $n = 1, k = 0$. $f(x) \equiv 0 \pmod p$ and $\nu_p\left(\frac{\partial f}{\partial X_j}(x)\right) = 0$, implies that $\frac{\partial f}{\partial X_j}(x)$ is unit. Then there exists a zero y such that $y \equiv x \pmod p$. □

Corollary 2.2.7. *For $p \neq 2$ and $f(X) = \sum a_{ij} X_i X_j$ with $a_{ij} = a_{ji}$ be quadratic form with coefficients in $\mathbb{Z}_p$ whose discriminant $\det(a_{ij})$ is invertible. If $a \in \mathbb{Z}_p$ then every primitive solution of equation $f(x) \equiv a \pmod p$ lifts to the solution in $\mathbb{Z}_p$.*

Proof. We have primitive solution of f. $f(X) = \sum a_{ij} X_i X_j$ is quadratic form with coefficients in $\mathbb{Z}_p$. Then $\frac{\partial f}{\partial X_i} = 2\sum_j a_{ij} X_j$, also $\det(a_{ij}) \not\equiv 0 \pmod p$ and x is primitive. Then for one of the $i,\quad \frac{\partial f}{\partial X_i} = 2\sum_j a_{ij} X_j$ is not multiple of p. i.e., $\frac{\partial f}{\partial X_i} \not\equiv 0 \pmod p$. Indirectly we have one of the partial derivative is non-zero means primitive zero is become simple zero f. Then by Corollary 2.2.6, we have solution in $\mathbb{Z}_p$. □

Note that $\det(a_{ij})$ is invertible means any row of matrix is not divisible by p. Each entry a_{ij} in $\frac{\partial f}{\partial X_i} = 2\sum_j a_{ij} X_j$ is from i^{th} row.

Corollary 2.2.8. *For $p = 2$, $f(X) = \sum a_{ij} X_i X_j$ with $a_{ij} = a_{ji}$ be quadratic form with coefficients in $\mathbb{Z}_2$. Let x be primitive solution of $f(x) \equiv a \pmod 8$ and $\det(a_{ij})$ is invertible. If x does not annihilate all the $\frac{\partial f}{\partial X_j} modulo 4$, then x can lifted as a solution in $\mathbb{Z}_p$.*

Proof. Here we have $p = 2$. By substituting $n = 3, k = 1$ in Theorem 2.2.5, we have solution $f(x) \equiv a \pmod 8$. $f(X) = \sum a_{ij} X_i X_j$ is quadratic form with coefficients in $\mathbb{Z}_2$. Then $\frac{\partial f}{\partial X_i} = 2\sum_j a_{ij} X_j$, also $\det(a_{ij}) \not\equiv 0 \pmod p$ and x is primitive. Then $\forall \quad i,\quad \frac{\partial f}{\partial X_i} = 2\sum_j a_{ij} X_j$ is multiple of 2 but not multiple of 4. i.e., $\frac{\partial f}{\partial X_i} \not\equiv 0 \pmod 4$. Indirectly we have one of the partial derivative is non-zero means primitive zero is become simple zero f. Then by Corollary 2.2.6, we have solution in $\mathbb{Z}_p$. □

2.3 The multiplicative group $\mathbb{Q}_p$

In this section, we will see that p-adic units can be defined as projective limit. Then exact sequence give some relation between U and $\mathbb{F}_p^*$,and as consequences $\mathbb{Q}_p$ contains $(p-1)^{th}$ roots of unity. Then further study for $U_1 = 1 + p\mathbb{Z}_p$, which is isomorphic to $\mathbb{Z}_p$ if $p \neq 2$ and isomorphic to $\{\pm 1\} \times U_2$. In last see squares in $\mathbb{Q}_p$.

2.3.1 Filtration of group of units

Let $U = \mathbb{Z}_p^*$ be the group of p-adic units. Define map

$$f_n : U \to (\mathbb{Z}_p/p^n\mathbb{Z}_p)^*,$$
$$u \mapsto u \pmod{p^n}$$

f_n is well defined, for any $u_1 = u_2 \in U$ and $u_1(u_2)^{-1} \in U$ then $u_1(u_2)^{-1} \pmod{p^n} \in (A_n)^*$ and $u_1 \pmod{p^n} = u_2 \pmod{p^n}$. Clearly, f_n is homomorphism, because for any $u_1, u_2 \in U$,

$$f_n(u_1u_2) = u_1u_2 \pmod{p^n} = (u_1 \pmod{p^n})\,(u_2 \pmod{p^n}) = f_n(u_1)f_n(u_2)$$

One can see that kernel of f_n is $U_n = 1 + p^n\mathbb{Z}_p$, where $n \in \mathbb{N}$. If we take $n = 1$, then U/U_1 is gives isomorphism with $\mathbb{F}_p^* = (A_1)^*$. Note that $\ldots U_n \subset U_{n-1} \subset \ldots U_2 \subset U_1 \subset U$. This means U_n forms decreasing sequence of subgroups of U. Now we want to show that projective limit of U/U_n is U. There are two ways to defining this, one is direct from projective limits of $\mathbb{Z}_p$ and another is abstract way by mapping $U/U_n \to U/U_{n-1}$. First we see by direct way. For all $n \in \mathbb{N}$, define the map $\xi_n : U_n \to \mathbb{Z}/p\mathbb{Z} = A_1$ as $\xi_n(1 + p^n x) := x \pmod{p}$.

Proposition 2.3.1. *For all $n \in \mathbb{N}$, the map ξ_n gives rise to an isomorphism of groups $U_n/U_{n+1} \to \mathbb{Z}/p\mathbb{Z} = A_1$.*

Proof. Its easy to see that the map ξ_n is well-defined and surjective. Now we want to prove that this map is homomorphism, We need to prove $\xi_n(a \cdot b) = \xi_n(a) + \xi_n(b)$, for $a, b \in U_n$. Take a and b to be $1 + p^n u_1$ and $1 + p^n u_2$, respectively. Then

$$\begin{aligned}
\xi_n(a \cdot b) &= \xi_n(1 + p^n(u_1 + u_2 + p^n(u_1u_2)) \\
&= (u_1 + u_2 + p^n(u_1u_2)) \pmod{p} \\
&= (u_1 + u_2) \pmod{p} \\
&= u_1 \pmod{p} + u_2 \pmod{p} \\
&= \xi_n(a) + \xi_n(b).
\end{aligned}$$

One can see that kernel is U_{n+1}, because if $a = 1 + p^n u_1 \in U_n$, and if u_1 is multiple of p, then image of a is zero in A_1. Then one can conclude that $U_n/U_{n+1} \cong A_1$, for any $n \in \mathbb{N}$. □

Proposition 2.3.2. *U/U_n isomorphic to $(A_n)^*$, $n \in \mathbb{N}$.*

Proof. Above proposition says that $U_n/U_{n+1} \cong \mathbb{Z}/p\mathbb{Z}$, which implies that order of U_n/U_{n+1} is p. Then its immediate that,

$$\#U_1/U_n = \#((U_1/U_2) \cdot (U_2/U_3) \cdots (U_{n-2}/U_{n-1}) \cdot (U_{n-1}/U_n)) = p^{n-1}.$$

From this we have $U/U_n = (U/U_1) \cdot (U_1/U_n)$, but we know cardinality of both (U/U_1) and (U_1/U_n). Then

$$\#U/U_n = \#(U/U_1)\#(U_1/U_n) = (p-1)(p^{n-1}) = p^n - p^{n-1}.$$

Interesting fact is that cardinality of $(A_n)^*$ is also $p^n - p^{n-1}$. Then recall that map f_n, which is injective and then become an isomorphism $U/U_n \cong (A_n)^*$. □

Now we have all ingredients to define projective limits directly.

Theorem 2.3.3. *The multiplicative group U is equal to $\varprojlim (U/U_n)$.*

Proof. We know that $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, and form above proposition,

$$\varprojlim (U/U_n) \cong \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^* = \left(\varprojlim \mathbb{Z}/p^n\mathbb{Z}\right)^* = (\mathbb{Z}_p)^* = U$$

□

Lemma 2.3.4. *Let $0 \to A \to E \to B \to 0$ be an exact sequence of commutative groups, also $\#A = a, \#B = b$ such that $(a,b) = 1$ and $C = \{x \in E | bx = 0\}$ is subgroup of E. Then show that $E = A \oplus C$ also, C is only subgroup of E which isomorphic to B.*

Proof. We have given that $(a,b) = 1$ i.e., there exists $r, s \in \mathbb{Z}$ such that $ar + bs = 1$. If $x \in A \cap C$ then $ax = bx = 0$ with $x = (ar+bs)x = 0$, which implies $A \cap C = \{0\}$. Every $x \in E$ can be written as $x = arx + bsx$, but $bC = 0$ and $bE \subset A$ because $bx = barx + b(bsx)$ then $bx = 0 + b(bsx)$ with $bsx \in A$, also $abE = 0$ then $arx \in C$. Hence we are done with $E = A \oplus C$. Now, if we restrict projection $E \to B$ on C then we know that $bC = 0$ and $\#B = b$, which gives isomorphism C onto B. If C' is other subgroup of E isomorphic to B, then $bC' = 0$. Hence $C' \subset C$ and by both groups having same order one can conclude that $C' = C$. □

Proposition 2.3.5. *p-adic units $U = V \times U_1$, where $V = \{x \in U | x^{p-1} = 1\}$ is unique subgroup of U which isomorphic to $\mathbb{F}_p^*$.*

Proof. To prove this we apply Lemma 2.3.4 on sort exact sequence,

$$1 \to U_1/U_n \to U/U_n \to \mathbb{F}_p^* \to 1,$$

because order of U_1/U_n is p^{n-1} and order of $\mathbb{F}_p^*$ is $p-1$. i.e,$(p^{n-1}, p-1) = 1$, also

$$U/U_n = U/U_1 \times U_1/U_n = U/U_1 \oplus U_1/U_n.$$

So that we can apply above lemma as following,

$$1 \to U_1/U_n \to U/U_1 \oplus U_1/U_n \to \mathbb{F}_p^* \to 1.$$

Since,

$$\varprojlim U/U_n = U \text{ and } \varprojlim U_1/U_n = U_1,$$

also, $U/U_1 \cong \mathbb{F}_p^*$ and we can see that the projective limit of U/U_1 is $(\mathbb{F}_p^*)'$ by identity map on $U/U_1 \to U/U_1$. Then one can think of map $U/U_n \to U/U_{n-1}$ which carries V_n isomorphically onto V_{n-1}. Finally,

$$\varprojlim V_n = \varprojlim U/U_1 = U/U_1 = (\mathbb{F}_p^*)',$$

by above projective limit we can conclude that U/U_n contains a unique subgroup V_n isomorphic to $\mathbb{F}_p^*$ with $U = V \times U_1 = (\mathbb{F}_p^*)' \times U_1$. □

Corollary 2.3.6. *The field $\mathbb{Q}_p$ contains $(p-1)^{th}$ roots of unity.*

Proof. Any non-zero element of $\mathbb{Q}_p$ can be written in terms of $p^n u$, where $n \in \mathbb{Z}$ and $u \in U$. From Proposition 2.3.5 we know that U is isomorphic to $V \times U_1$, and $V = \{x \in U | x^{p-1} = 1\}$. i.e., $\mathbb{Z}_p$ itself contains $(p-1)^{th}$ roots of unity, which implies $\mathbb{Q}_p$ contains $(p-1)^{th}$ roots of unity. □

2.3.2 Structure of U_1 in terms of $\mathbb{Z}_p$

Lemma 2.3.7. *Let x be an element of $U_n \setminus U_{n+1}$. If $p \neq 2$ then $n \geq 1$ and if $p = 2$ then $n \geq 2$. Then $x^p \in U_{n+1} \setminus U_{n+2}$.*

Proof. Take x from $U_n \setminus U_{n+1}$, then $x = 1 + p^n u$ where $u \in \mathbb{Z}_p$ with $u \not\equiv 0 \pmod p$ implies $u \in U$. From binomial formula by taking power p,

$$\begin{aligned} x^p &= (1 + p^n u)^p \\ &= 1 + up^{n+1} + u^2 p^{n+2} + \ldots + u^p p^{np} \end{aligned}$$

Here the exponents in terms not written are $\geq 2n+1$, also $np \geq n+2$. By taking modulo p^{n+2},

$$x^p \equiv 1 + p^{n+1} u \pmod{p^{n+2}}$$

Hence, $x^p \in U_{n+1} \setminus U_{n+2}$. □

Proposition 2.3.8. *U_1 is isomorphic to $\mathbb{Z}_p$ if $p \neq 2$, and when $p = 2$, $U_1 = \{\pm 1\} \times U_2$ where U_2 is isomorphic to $\mathbb{Z}_2$.*

Proof. First we prove for $p \neq 2$. Let x be an element from $U_1 \setminus U_2$. If $x = 1 + p$, then by Lemma 2.3.7 $x^p \in U_2 \setminus U_3$ and then $x^{p^n} \in U_{n+1} \setminus U_{n+2}$. Take image of x in U_1/U_n as x_n, then

$$\begin{aligned} x^{p^{n-1}} &= (1 + p)^{p^{n-1}} \\ &= 1 + p^n + \ldots + p^{p^{n-1}} \end{aligned}$$

Then $x_n^{p^{n-1}} = 1$, but note that $x_n^{p^{n-2}} \neq 1$ because if power is $n-2$ then second term of binomial formula is exponent of p^{n-1} and that sum won't give 1 in U_1/U_n. We know that U_1/U_n is group of order p^{n-1}, which implies that x_n is generator of cyclic group U_1/U_n. Now define map,

$$\begin{aligned} \lambda_{n,x} \quad : \quad & A_{n-1} \to U_1/U_n \\ & z_{n-1} \mapsto x_n^{z_{n-1}}. \end{aligned}$$

Its clear that map is well-defined, also forms homomorphism given by,

$$\lambda_{n,x}(z_{n-1} + y_{n-1}) = x_n^{z_{n-1}+y_{n-1}} = x_n^{z_{1,n-1}} \cdot x_n^{y_{n-1}} = \lambda_{n,x}(z_{n-1})\lambda_{n,x}(y_{n-1}).$$

Now recall map $\varphi_n : A_n \to A_{n-1}$ in starting of this Chapter. Take $z_n \in A_n$ then by map φ_n we get,

$$\varphi_n(z_n) = z_{n-1} \in A_{n-1}.$$

We defining map $\mu_n : U_1/U_{n+1} \to U_1/U_n$. Now, we have all ingredients to prove this result. Now applying,

$$\lambda_{n+1,x} : A_n \to U_1/U_{n+1},$$

which gives,

$$\lambda_{n+1,x}(z_n) = x_{n+1}^{z_n}.$$

Further applying $\mu_n : U_1/U_{n+1} \to U_1/U_n$ on $x_{n+1}^{z_n}$, we get following,

$$\mu_n(x_{n+1}^{z_n}) = x_n^{z_{n-1}} = \mu_n(\lambda_{n+1,x}(z_n)),$$

but by φ_n we got z_{n-1}, then applying $\lambda_{n,x}$ on z_{n-1} we get $x_n^{z_{n-1}} = \lambda_{n,x}(\varphi_n(z_n))$. Its clear that

$$\mu_n(\lambda_{n+1,x}(z_n)) = x_n^{z_{n-1}} = \lambda_{n,x}(\varphi_n(z_n)).$$

From this one can define isomorphism,

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^{n-1}\mathbb{Z} \text{ onto } U_1 = \varprojlim U_1/U_n.$$

Hence we are done for $p \neq 2$. Now if $p = 2$ then one can chose $x \in U_2 \setminus U_3$, with this we get $x \equiv 5 \pmod 8$. By defining map,

$$\lambda_{n,x} : \mathbb{Z}/2^{n-2}\mathbb{Z} \to U_2/U_n$$

by similar way one can see that,

$$\mathbb{Z}_2 = \varprojlim \mathbb{Z}/p^{n-2}\mathbb{Z} \text{ onto } U_2 = \varprojlim U_2/U_n.$$

Also we have homomorphism $\xi_1 : U_1 \to U_1/U_2$ but $U_1/U_2 \cong \mathbb{Z}/2\mathbb{Z}$, further an isomorphism of $\{\pm 1\}$ onto $\mathbb{Z}/2\mathbb{Z}$ gives $U_1 = \{\pm 1\} \times U_2$. □

Theorem 2.3.9. *Prove that if $p \neq 2$ then multiplicative group $\mathbb{Q}_p^* \cong \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}\ (p-1)\mathbb{Z}$, if $p = 2$ then isomorphic to $\mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$.*

Proof. We know that every non-zero element of $\mathbb{Q}_p^*$ can be written uniquely as $x = p^n u$, where $n \in \mathbb{Z}$ and $u \in U$. Hence by map $x \mapsto (\nu_p(x), u)$ gives isomorphism between $\mathbb{Q}_p^*$ and $\mathbb{Z} \times U$. By Proposition 2.3.5 we know that $U = V \times U_1$ and V is is cyclic group of order $p-1$. From Proposition 2.3.8 U_1 is isomorphic to $\mathbb{Z}_p$. Then $\mathbb{Q}_p^* \cong \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$. If $p = 2$ then first $U = U_1$ and Proposition 2.3.8 $U_1 = \{\pm 1\} \times U_2$ and $U_2 \cong \mathbb{Z}_2$. Hence $\mathbb{Q}_p^* \cong \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$. □

2.3.3 Squares in multiplicative group $\mathbb{Q}_p^*$

Theorem 2.3.10. *If $p \neq 2$ and let $x = p^n u$ be an element of $\mathbb{Q}_p^*$ where $n \in \mathbb{Z}$ and $u \in U$. For x to be square it is necessary and sufficient that n is even and image $\overline{u}$ of u in $\mathbb{F}_p^* = U/U_1$ is square.*

Proof. Its given that $x = p^n u$. From Proposition 2.3.5 we know that $U = V \times U_1$, then by decomposing $u \in U$ to $u = vu_1$ with $v \in V$ and $u_1 \in U_1$. From Theorem 2.3.9, decomposing $\mathbb{Q}_p^* \cong \mathbb{Z} \times V \times U_1$, but $U_1 \cong \mathbb{Z}_p$. By squaring $\mathbb{Q}_p^*$, we have $\mathbb{Q}_p^{*2} \cong 2\mathbb{Z} \times \mathbb{F}_p^{*2} \times 2\mathbb{Z}_p$ ($\because$ $\mathbb{Q}_P^*$ and $\mathbb{F}_p^*$ both multiplicative groups, also $\mathbb{Z}$ and $\mathbb{Z}_p$ both additive group, but $2\mathbb{Z}_p = \mathbb{Z}_p$, because 2 is invertible in $\mathbb{Z}_p$. Hence by isomorphism $\mathbb{Z}_p \cong U_1$ all elements of U_1 are squares, then we have $\mathbb{Q}_p^{*2} \cong 2\mathbb{Z} \times \mathbb{F}_p^{*2} \times U_1$. Now one can see that by map $x \mapsto (\nu_p(x), u), x \in \mathbb{Q}_p$ is square if n even and image $\overline{u}$ of u in $\mathbb{F}_p^* = U/U_1$ is square. i.e, Legendre symbol $\left(\frac{\overline{u}}{p}\right)$ of $\overline{u}$ is equal to 1. □

Corollary 2.3.11. *If $p \neq 2$, then multiplicative group $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ is group of type $(2, 2)$. It has representatives $\{1, p, u, up\}$ where $u \in U$ such that $\left(\frac{u}{p}\right) = -1$*

Proof. From Theorem 2.3.10, its clear that $\mathbb{Q}_p^* \cong \mathbb{Z} \times \mathbb{F}_p^* \times \mathbb{Z}_p$ and $\mathbb{Q}_p^{*2} \cong 2\mathbb{Z} \times \mathbb{F}_p^{*2} \times \mathbb{Z}_p (\because 2\mathbb{Z}_p = \mathbb{Z}_p)$, but $\mathbb{Z}_p \cong U_1$,

$$\frac{\mathbb{Q}_p^*}{\mathbb{Q}_p^{*2}} \cong \underbrace{\frac{\mathbb{Z}}{2\mathbb{Z}}}_{\nu_p} \times \underbrace{\frac{\mathbb{F}_p^*}{\mathbb{F}_p^{*2}}}_{u} \times \frac{U_1}{U_1}.$$

From that we get,

$$\#\frac{\mathbb{Q}_p^*}{\mathbb{Q}_p^{*2}} = \#\frac{\mathbb{Z}}{2\mathbb{Z}} \times \#\frac{\mathbb{F}_p^*}{\mathbb{F}_p^{*2}} \times \#\frac{U_1}{U_1}.$$

To see representatives of $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, consider map $x \mapsto (\nu_p(x), u)$. From this take valuation such that an element 1 which has valuation zero and other p which has non-zero valuation. i.e., we can take $\{1, p\}$. Now, for squares consider an element 1 in $\mathbb{F}_p^*$ which is square. i.e, $\left(\frac{1}{p}\right) = 1$ and other element as non-square u such that $\left(\frac{u}{p}\right) = -1$, which implies we can take $\{1, u\}$ Then one can see that of $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ is group of type $(2, 2)$ and has representatives $\{1, p\} \times \{1, u\} = \{1, p, u, pu\}$. □

Theorem 2.3.12. *An element $x = p^n u$ of $\mathbb{Q}_2^*$ to be a square it is necessary and sufficient that n is even and $u \equiv 1 \pmod 8$.*

Proof. We know that we can decomposing $U = \{\pm 1\} \times U_2$, and from that u is square if and only if $u \in U_2$ with square in U_2. From Proposition 2.3.8 isomorphism $\mathbb{Z}_2 \cong U_2$ carries $2^n\mathbb{Z}_2$ onto U_{n+2}. Now by taking $n = 1$ one can see that set of squares of U_2 is same as to U_3, because, squares in $\mathbb{Z}_2$ is $2\mathbb{Z}_2$, but squares in U_2 is U_3. Note the fact that in Proposition2.3.8, we took $x \in U_2 \setminus U_3$, then its clear that $x^2 \in U_3 \setminus U_4$. By definition of $U_3 = 1 + 2^3\mathbb{Z}_2$, its clear that if $x \in U_2$ is square if and only if $x^2 \equiv 1 \pmod 8$. Hence we proved. □

Proposition 2.3.13. *Prove that if $p = 2$, then U/U_3 is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Proof. First, note that when $p = 2$ then $U = U_1$, then one can see that we can define homomorphism $U_1/U_2 \times U_2/U_3$ onto $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which is same as saying $U/U_2 \times U_2/U_3$ onto $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Finally, define homomorphism $f_1 : U/U_2 \to \mathbb{Z}/2\mathbb{Z}$ as follows,

$$f_1(x) \equiv \frac{x-1}{2} \pmod 2 = \begin{cases} 0 & \text{if } x \equiv 1 \pmod 4 \\ 1 & \text{if } x \equiv -1 \pmod 4 \end{cases} \tag{2.1}$$

and define another homomorphism $f_2 : U_2/U_3 \to \mathbb{Z}/2\mathbb{Z}$ as follows,

$$f_2(x) \equiv \frac{x^2-1}{8} \pmod 2 = \begin{cases} 0 & \text{if } x \equiv \pm 1 \pmod 8 \\ 1 & \text{if } x \equiv \pm 5 \pmod 8 \end{cases} \tag{2.2}$$

Then the pair (f_1, f_2) defines isomorphism $U/U_2 \times U_2/U_3 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which is U/U_3 onto $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. i.e., A 2-adic unit x is square if and only if $f_1(x)$ and $f_2(x)$ both zero. □

Corollary 2.3.14. *The multiplicative group $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ is of type $(2, 2, 2)$. It has representatives $\{\pm 1, \pm 2, \pm 5, \pm 10\}$.*

Proof. For $p = 2$, $\mathbb{Q}_2^* \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \cong U_2$. By squaring $\mathbb{Q}_2^*$, we get $\mathbb{Q}_2^{*2} \cong 2\mathbb{Z} \times 2\mathbb{Z}/2/\mathbb{Z} \times 2\mathbb{Z}_2$. Then

$$\frac{\mathbb{Q}_2^*}{\mathbb{Q}_2^{*2}} \cong \underbrace{\frac{\mathbb{Z}}{2\mathbb{Z}}}_{\nu_p} \times \underbrace{\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}_2}{2\mathbb{Z}_p}}_{\cong U/U_3}. \tag{2.3}$$

As in equation (2.3), recall map $x \mapsto (\nu_p(x), u)$. Then Theorem 2.3.12 says that $u \equiv 1 \pmod 8$ and set of squares of U_2 is equal to U_3, then we consider U_2/U_3 which is isomorphic to $\mathbb{Z}_2/2\mathbb{Z}_2$, where $\mathbb{Z}_2/2\mathbb{Z}_2 \cong \mathbb{Z}/2\mathbb{Z}$ Also when $p = 2$ then $U = U_1$, then $U_1/U_2 \cong \mathbb{Z}/2\mathbb{Z}$ is same as $U/U_2 \cong \mathbb{Z}/2\mathbb{Z}$. From Proposition 2.3.13, $U/U_3 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. To see representatives of U/U_3, we take element 1, as square and -1 as non-square. Also, element 1 as unit in U, and 5 as element in U_2 but not in U_3. Then we have $\{+1, -1\} \times \{1, 5\} = \{\pm 1, \pm 5\}$. Finally, for valuation we can take element 1 which has valuation zero, and take element 2 which has non-zero valuation. Then we can say that $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ is type of $(2, 2, 2)$, which has for representatives $\{1, 2\} \times \{\pm 1, \pm 5\} = \{\pm 1, \pm 2, \pm 5, \pm 10\}$. $\square$

Chapter 3

Hilbert Symbol

In this chapter, we shall see some important properties of quadratic forms in 3 variables over $\mathbb{R}$ and $\mathbb{Q}_p$, where p is prime number. Though out this chapter, we let $\mathbb{K}$ to denote either $\mathbb{R}$ or $\mathbb{Q}_p$.

3.1 Local properties

In this section, we shall first define the Hilbert symbol and later we produce some properties of it.

Definition 23. *A function* $(\ ,\ ) : \mathbb{K} \times \mathbb{K} \to \{\pm 1\}$ *is defined as, for any* $a, b \in \mathbb{K}^*$*,*

$$(a, b) = \begin{cases} 1, & \text{if } z^2 - ax^2 - by^2 = 0 \text{ has a non-zero solution in } \mathbb{K}^3, \\ -1 & \text{otherwise.} \end{cases}$$

The number $(a, b) = \pm 1$ *is called Hilbert Symbol of* a *and* b *relative to* $\mathbb{K}$*.*

Lemma 3.1.1. *The Hilbert symbol* (a, b) *does not change if* a *and* b *are multiplied by squares.*

Proof. If a quadratic form $z^2 - ax^2 - by^2 = 0$ has a non-zero solution (z', x', y'), then the solution of the quadratic form $z^2 - ac^2x^2 - bd^2y^2 = 0$ is (z', cx', dy'), where $c, d \in \mathbb{K}$. □

Thus, it is suffices to consider the Hilbert symbol when neither a nor b is a square. By Lemma 3.1.1, the Hilbert symbol is a function on $\mathbb{K}^*/\mathbb{K}^{*2}$, *i.e.*.

$$(\ ,\ ) : \mathbb{K}^*/\mathbb{K}^{*2} \times \mathbb{K}^*/\mathbb{K}^{*2} \to \{\pm 1\}.$$

Definition 24. *Let* $\mathbb{K}$ *be any field, then for any* $\sqrt{a} \notin \mathbb{K}^*$*,* $\mathbb{K}_a = \mathbb{K}(\sqrt{a})$ *is the quadratic extension of* $\mathbb{K}$*, where* $\mathbb{K}_a$ *is the smallest extension of* $\mathbb{K}$ *containing* $\sqrt{a}$*. Also,* $\mathbb{K}_a = \{x + \sqrt{a}y |\ x, y \in \mathbb{K}\}$*.*

If $\mathbb{K}_a$ is quadratic extension and $x + \sqrt{a}y = f \in \mathbb{K}_a$ then we define norm of f as
$N(f) = (x + \sqrt{a}y)(x - \sqrt{a}y) = x^2 - ay^2$.

Proposition 3.1.2. *Let b be in $\mathbb{K}^*$ with $\sqrt{b} \notin \mathbb{K}^*$ and $\mathbb{K}_b = \mathbb{K}(\sqrt{b})$, then $N\mathbb{K}_b^*$ forms group of norms of elements of $\mathbb{K}_b^*$.*

Proof. $\mathbb{K}_b^*$ is multiplicative group and $N\mathbb{K}_b^* = \{N(x) \mid x = y + \sqrt{b}z \ \& \ y, z \in \mathbb{K}_b^*\}$. Thus, it is clear. □

Proposition 3.1.3. *Let a,b in $\mathbb{K}^*$, and $\mathbb{K}_b = \mathbb{K}(\sqrt{b})$, then for Hilbert symbol $(a, b) = 1$, it is necessary and sufficient that $a \in N\mathbb{K}_b^*$.*

Proof. We have two cases, first when b is square and second is when b is non-square.

i) When b is square of an element $c \in \mathbb{K}^*$. Now, quadratic form $z^2 - ax^2 - by^2 = 0$ has $(c, 0, 1)$ is non-trivial solution. Hence, $(a, b) = 1$. Also, its easy to see that in this case $\mathbb{K}_b = \mathbb{K}$ as well as $N\mathbb{K}_b^* = \mathbb{K}^*$.

ii) When $b \in \mathbb{K}^*$ but b is not square of any element, then $\mathbb{K}_b$ is quadratic extension over $\mathbb{K}$. Since, every element of $z \in \mathbb{K}_b$ can be written as $z = h + \sqrt{b}k$ with $h, k \in \mathbb{K}$ and $N(z) = h^2 - bk^2$. If $a \in N\mathbb{K}_b^*$, there exists $y, z \in \mathbb{K}$ such that $a = z^2 - by^2$. This implies that quadratic form $z^2 - ax^2 - by^2 = 0$ has non trivial zero $(z, 1, y)$. Thus, $(a, b) = 1$.

Conversely, if $(a, b) = 1$, implies that quadratic form $z^2 - ax^2 - by^2 = 0$ has non-trivial solution. We can say that x is non zero, otherwise b would be square. Then, its clear that $N(\frac{z}{x} + \sqrt{b}\frac{y}{x}) = a$. □

3.1.1 Properties of Hilbert symbol

Lemma 3.1.4. *Hilbert symbol satisfies following. Let $a, b, c \in \mathbb{K}^*$.*

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

ii) $(a, c^2) = 1$.

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

iv) $(a, 1 - a) = 1$, *if* $a \neq 1$.

v) $(a, b) = 1 \Rightarrow (ac, b) = (c, b)$,

vi) $(a, b) = (a, -ab) = (a, (1 - a)b)$, *if* $a \neq 1$.

Proof. i) $(a, b) = (b, a)$
If a quadratic form $z^2 - ax^2 - by^2 = 0$ has a non-zero solution (h, k, l), then $z^2 - bx^2 - ay^2 = 0$ has the non-zero solution (h, l, k). This implies that $(a, b) = (b, a)$.

ii) $(a, c^2) = 1$

By first case of Proposition 3.1.3, quadratic form $z^2 - ax^2 - by^2 = z^2 - ax^2 - c^2y^2 = 0$ has solution $(c, 0, 1)$ is solution. Thus, $(a, b) = (a, c^2) = 1$. It is saying that, Hilbert symbol of a and b relative to $\mathbb{K}$ is always 1 if any one of them is square.

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

If $b = -a$ then quadratic form $z^2 - ax^2 - by^2 = z^2 - ax^2 + ay^2 = 0$ has non trivial solution $(0, 1, 1)$, which implies that $(a, -a) = 1$.

iv) $(a, 1 - a) = 1$, if $a \neq 1$.

If $b = 1 - a$ then quadratic form $z^2 - ax^2 - by^2 = z^2 - ax^2 - y^2 + ay^2 = 0$ has non trivial solution $(1, 1, 1)$. Thus, $(a, 1 - a) = 1$.

v) $(a, b) = 1 \Rightarrow (ac, b) = (c, b)$,

It is given that $(a, b) = 1$, then by converse part of Proposition 3.1.3 its clear that $a \in N\mathbb{K}_b^*$. If $c \in N\mathbb{K}_b^*$ then $ac \in N\mathbb{K}_b^*$, because, we know that $z_1, z_2 \in \mathbb{K}_b^*$ such that $N(z_1) = a$ and $N(z_2) = c$, then one can find $z_3 \in \mathbb{K}_b^*$ such that $N(z_3) = ac$. Also, if $ac \in \mathbb{K}_b^*$, then for some $z_4 \in \mathbb{K}_b^*$, $N(z_4) = ac$ then $N(z_4/z_1) = c$, thus $c \in N\mathbb{K}_b^*$. This proves $(ac, b) = (c, b)$.

vi) $(a, b) = (a, -ab) = (a, (1 - a)b)$, if $a \neq 1$.

It is quite easy to prove, because it is from above property only, We know that $(a, -a) = 1$ then $(a, -ab) = (a, b)$, also $(a, 1 - a) = 1$ then $(a, (1 - a)b) = (a, b)$.

□

3.1.2 Computation of (a, b)

Theorem 3.1.5. *If $\mathbb{K} = \mathbb{R}$, then,*

$$(a, b) = \begin{cases} 1, & \text{if } a \text{ or } b \text{ is } > 0, \\ -1 & \text{if } a \text{ and } b \text{ both } < 0. \end{cases}$$

Proof. Since $\mathbb{K} = \mathbb{R}$, the representatives for $\mathbb{R}^*/\mathbb{R}^{*2}$ are $\{1, -1\}$. Since 1 is a square, we see that $(1, 1) = (1, -1) = (-1, 1) = 1$. The Hilbert symbol $(-1, -1)$ is -1, since $z^2 + x^2 + y^2$ cannot represent zero non-trivially. □

Lemma 3.1.6. *Let $b \in U$ be a p-adic unit. If the quadratic form $z^2 - px^2 - by^2 = 0$ has a non-trivial solution in $\mathbb{Q}_p$, then it has a solution (z, x, y) such that $z, y \in U$ and $x \in \mathbb{Z}_p$.*

Proof. By Proposition 2.2.3, the given equation has a primitive solution (z, x, y). We will show by contradiction that this solution has the desired property.

Suppose, it does not have such property, then we would have either $y \equiv 0 \pmod{p}$ or $z \equiv 0 \pmod{p}$. Let, $z \equiv 0 \pmod{p}$, then by taking modulo p of the equation $z^2 - px^2 - by^2 = 0$ gives $z^2 - by^2 \equiv 0 \pmod{p}$, but we know that $b \not\equiv 0 \pmod{p}$, which implies y and z both multiple of p. This gives $px^2 \equiv 0 \pmod{p^2}$. Then, $x \equiv 0 \pmod{p}$. This means that any of z, x, y is not invertible then it is not primitive solution, which contradicts to our assumption for y or z is congruent to modulo p. Hence, if equation has non-trivial solution if there exists solution with y, z is invertible $(i.e.\ y, z \in U)$. □

Theorem 3.1.7. *If $\mathbb{K} = \mathbb{Q}_p$, and let $a, b \in \mathbb{Q}_p$, such that $a = p^h u, b = p^k v$, where u, v are p-adic units. Then,*

i) for $p \neq 2$:

$$(a, b) = (-1)^{hk\epsilon(p)} \left(\frac{u}{p}\right)^k \left(\frac{v}{p}\right)^h, \tag{3.1}$$

ii) for $p = 2$,

$$(a, b) = (-1)^{\epsilon(u)\epsilon(v)+h\omega(v)+k\omega(u)}. \tag{3.2}$$

[Recall that $\left(\frac{u}{p}\right)$ denotes the Legendre symbol $\left(\frac{\overline{u}}{p}\right)$, where $\overline{u}$ is the image of u by the homomorphism $U \to \mathbb{F}_p^*$ of reduction modulo p. As for $\epsilon(u)$ and $\omega(u)$ denote class modulo 2 of $\frac{u-1}{2}$ and $\frac{u^2-1}{8}$ respectively.]

Proof. As we know that for prime $p = 2$, case differs everywhere. So we suppose first prove for $p \neq 2$.

i) For $p \neq 2$:
In equation 3.1, exponents come in only by their residue modulo 2. Also, we are considering Hilbert symbol only on $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, which means, Hilbert symbol depends only on modulo $\mathbb{Q}_p^{*2}$. Since, representative of $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ is $\{1, p, u, up\}$, where $0 < u \leq p-1$ is any fixed non square($i.e.$ Legendre symbol of u is not equal to 1). It is clear that by representatives we have $4 \times 4 = 16$ cases, but from Lemma 3.1.4 it is reduces to only following three cases.

$$a)\ (u, u) = (u, v) \qquad b)\ (p, u) \qquad c)\ (pu, pu) = (pu, pv),$$

a) We know that $a = p^h u, b = p^k v$. To consider case (u, u) take $h = 0, k = 0$, because then, $(a, b) = (u, v) = 1$. By Corollary 1.2.5, it is clear that quadratic equation $z^2 - ux^2 - vy^2 = 0$ has non-trivial solution modulo p. By Corollary 3.1.6, it is easy to see that one of the partial derivative is nonzero and discriminant of this quadratic equation is p-adic unit. Finally, by Hensel's lemma we can lift to the solution in $\mathbb{Z}_p$. Thus, $(u, v) = 1$.

b) Now for (pu, v), by taking $h = 1, k = 0$ we get $a = pu, b = v$ $i.e.$ $(a, b) = (pu, v)$. Since, from above proof of $a)$ it is clear that $(u, v) = 1$, and from fifth property Lemma 3.1.4, one can see that $(pu, v) = (p, u)$. So we have to prove that $(p, v) = \left(\frac{v}{p}\right)$. Take quadratic equation $f = z^2 - px^2 - vy^2 = 0$. It is easy to see that if v is square then $(p, v) = 1 = \left(\frac{v}{p}\right)$, otherwise $\left(\frac{v}{p}\right) = -1$. Then Lemma 3.1.6, shows that equation $z^2 - px^2 - vy^2 = 0$ does not have non-trivial zero, which implies that $(p, v) = -1$.

c) In last case of $p \neq 2$, by taking $h = k = 1$, we get $(a, b) = (pu, pv)$ and

$$(pu, pv) = (-1)^{(p-2)/2} \left(\frac{u}{p}\right) \left(\frac{v}{p}\right).$$

By fifth property of Lemma 3.1.4,

$$(pu, pv) = (pu, -p^2uv) = (pu, -uv),$$

but just now we proved that $(pu, v) = (p, v) = \left(\frac{v}{p}\right)$, then $(pu, pv) = (pu, -uv) = \left(\frac{-uv}{p}\right)$ and we know that $u, v \in U$, which means $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. Now it is easy to see that if -1 is square modulo p, then $(pu, pv) = 1$, otherwise $(pu, pv) = -1$.

Now we prove it for $p = 2$.

ii) For $p = 2$,

$$(a, b) = (-1)^{\epsilon(u)\epsilon(v) + h\omega(v) + k\omega(u)}. \tag{3.3}$$

a) We know that $a = 2^h u, b = 2^k v$. To consider case (u, u) take $h = k = 0$, because then,

$$(a, b) = (u, v) = \begin{cases} 1, & \text{if } u \text{ or } v \equiv 1 \pmod 4 \\ -1, & \text{otherwise .} \end{cases}$$

First case, $u \equiv 1 \pmod 4$ and $v \equiv -1 \pmod 4$, If u is square then $u \equiv 1 \pmod 8$, we already know that if one of them is square then $(u, v) = 1$. If u is non square, $i.e.$ $u \equiv 5 \pmod 8$ and $v \equiv -1 \pmod 4$, then we have $u + 4v \equiv 1 \pmod 8$ which implies $u + 4v$ is square. Then there is $w \in U$ such that $w^2 = u + 4v$ and $(w, 1, 2)$ is solution of $z^2 - ux^2 - vy^2 = 0 \Rightarrow (u, v) = 1$.

In second case $u \equiv v \equiv -1 \pmod 4$ and (z, x, y) is primitive solution of $z^2 - ux^2 - vy^2 = 0$ then $z^2 + x^2 + y^2 \equiv 0 \pmod 4$. Since, $\bar{0}$ and $\bar{1}$ are only squares in $\mathbb{Z}/4\mathbb{Z} \Rightarrow z, x, y \equiv 0 \pmod 2$. This contradicts to primitivity. Thus, $(u, v) = -1$.

b) Now, $a = 2^h u, b = 2^k v$. To consider case $(2u, u)$ take $h = 1, k = 0$ then we have to check,

$$(a, b) = (-1)^{\epsilon(u)\epsilon(v)+h\omega(v)},$$

First, let's show that $(2, v) = (-1)^{\omega(v)}$. $i.e.(2, v) = 1 \iff v \equiv \pm 1 \pmod 8$. If $(2, v) = 1$, by above Lemma 3.1.6 there is $x, y, z \in \mathbb{Z}_2$ such that $y, z \in {\mathbb{Z}_2}^*$ with,

$$z^2 - 2x^2vy^2 = 0, y^2, z^2 \in {\mathbb{Z}_2}^{*2}, \Rightarrow y^2 \equiv z^2 \equiv 1 \pmod 8, \tag{3.4}$$

$$\Rightarrow 1 - 2x^2 - v \equiv 0 \pmod 8 \tag{3.5}$$

Since, $\bar{0}, \bar{1}$ and $\bar{4}$ are squares in $\mathbb{Z}/8\mathbb{Z}$, which means that $v \equiv \pm 1 \pmod 8$. Conversely, if $v \equiv 1 \pmod 8$ and v is square then $(2, v) = 1$. If $v \equiv -1 \pmod 8$ then $z^2 - 2x^2 - vy^2 = 0$ has $(1, 1, 1)$ solution for modulo 8. It is easy to see that by Hensel's lemma we can lift solution in $\mathbb{Z}_2$. Thus, $(2, v) = 1$. Next, $(2u, v) = (2, v)(u, v)$. By one of the property of Hilbert symbol, its clear that $(2u, v) = (2, v)(u, v)$ is true if $(2, v) = 1$ or $(u, v) = 1$. The remaining case is $(2, v) = (u, v) = -1$, $i.e.$ $v \equiv 3 \pmod 8$ and $u \equiv 3$ or $-1 \pmod 8$, after multiplying u and v by squares, we can suppose that $u = -1, v = 3$ for equation $z^2 + 2x^2 - 3y^2 = 0$ and $u = 3, v = -5$ for equation $z^2 - 6x^2 + 5y^2 = 0$, both equations have solution $(1, 1, 1)$; thus we have $(2u, v) = 1$.

c) Finally, take $h = k = 1$,

$$(a, b) = (2u, 2v) = (-1)^{\epsilon(u)\epsilon(v)+h\omega(v)+k\omega(u)}. \tag{3.6}$$

Now, last property of Hilbert symbol shows that,

$$(2u, 2v) = (2u, -4uv) = (2u, -uv),$$

but, just now we have seen that,

$$(2u, 2v) = (-1)^{\epsilon(u)\epsilon(-uv)+\omega(-uv)}$$

Since, $\epsilon(-1) = 1, \omega(-1) = 0$ and $\epsilon(u)(1 + \epsilon(u)) = 0$. Also, $\epsilon(-uv) = \epsilon(u) + \epsilon(-1) + \epsilon(v)$, which proves the theorem.

□

Theorem 3.1.8. *Hilbert symbol is a non-degenerate bilinear form on the vector space $\mathbb{K}^*/\mathbb{K}^{*2}$ over $\mathbb{F}_2$.*

Proof. We first prove for $p \neq 2$, then prove for $p = 2$.

i) $p \neq 2$,
Its clear that formula itself giving Hilbert symbol (a, b) symbol is bilinear; to prove non-degeneracy it is suffices exhibit, for all $a \in \mathbb{K}^*/\mathbb{K}^{*2}$ distinct form neutral element b such that $(a, b) = -1$. We have four representatives for $\mathbb{Q}^*/\mathbb{Q}^{*2}$, then we can take $a = p, u$ or up with $u \in U$, such that $\left(\frac{u}{p}\right) = -1$; then we choose for b respectively, u, p and up.

ii) $p = 2$,
The bi-linearity of Hilbert symbol (a, b) follows from the formula giving this symbol (ϵ and ω are homomorphisms). For non-degeneracy is checked on the representatives $\{u, 2u\}$ with $u = 1, 5, -1$ or 5. Indeed, we have following,

$$(5, 2u) = -1 \text{ and } (-1, -1) = (-1, -5) = -1.$$

□

Corollary 3.1.9. *If b is not a square, the group $N\mathbb{K}_b^*$ is a group of index 2 in $\mathbb{K}^*$.*

Proof. Define map $\phi_b : \mathbb{K}^* \to \{\pm 1\}$, by $\phi_b(a) = (a, b)$. It is easy to see that its a homomorphism and it has kernel $N\mathbb{K}_b^*$. Since, (a, b) is non-degenerate, it is surjective. Hence, first isomorphism theorem, map ϕ_b defines an isomorphism of $\mathbb{K}/N\mathbb{K}_b^*$ onto $\{\pm 1\}$. Thus, index is equal to two follows. □

3.2 Global properties

This section makes use of the embedding of $\mathbb{Q}$ into $\mathbb{Q}_p$, for all primes p. First, we see important product formula of Hilbert symbol for almost all primes p. After that we will see the existence of rational numbers with given Hilbert symbols. In last, two important theorems, first one is Approximation theorem and second one is Dirichlet theorem. If $a, b \in \mathbb{Q}^*$, then $(a, b)_p$ denotes the Hilbert symbol of their images in $\mathbb{Q}_p$ (also, $(a, b)_\infty$ for images in $\mathbb{R}$). Let V be a set of all primes union with symbol ∞, and $\mathbb{Q}_\infty$ is equal to $\mathbb{R}$, hence, $\mathbb{Q}$ is dense in $\mathbb{Q}_v$ for all $v \in V$.

3.2.1 Product formula of Hilbert symbol

Following theorem is computation of results of previous theorem for different cases.

Theorem 3.2.1. *If $a, b \in \mathbb{Q}^*$, then $(a, b)_p = 1$ for all the elements of V except a finite number (i.e. for almost all $v \in V$) and*

$$\prod_{v \in V} (a, b)_v = 1.$$

Proof. For any two a, b in the form $p^h u, p^k v$ respectively, where u and v are p-adic units we have the following:

i) for $p \neq 2$,
$$(a, b) = (-1)^{hk\epsilon(p)} \left(\frac{u}{p}\right)^k \left(\frac{v}{p}\right)^h, \tag{3.7}$$

ii) for $p = 2$,
$$(a, b) = (-1)^{\epsilon(u)\epsilon(v)+h\omega(v)+k\omega(u)}. \tag{3.8}$$

It suffices to prove the theorem for a, b equal to -1 or p a prime, by the bi-linearity of Hilbert symbol. This can be done via following three cases,

1) $a = -1, b = -1$.
One can note form Theorem 3.1.5 that Hilbert symbol $(-1, -1)_\infty = -1$ as well as $(a, b)_2 = -1$, also $(a, b)_v = 1$, for all $v \neq 2, \infty$. Thus the product is clear.

2) $a = -1, b = q$ with q is prime.
If $q = 2$, then one has $(-1, 2)_v = 1$ for all $v \in V$. If $q \neq 2$ then $(-1, q)_v = 1$, finally if $v \neq 2, q$ and $(-1, q)_2 = (-1, q)_q = (-1)^{\epsilon(q)}$. One can see that product is equal to 1.

3) $a = p, b = q$ with p, q primes. To prove this we consider three cases as following:

case -1) If $p = q$,
$$(p, q) = (p, p) = \begin{cases} 1, & \text{if } -1 \text{ is square modulo } p, \\ -1, & \text{otherwise }. \end{cases}$$
$(p, p) = (p, -p)(p, p) = (p, -p^2) = (p, -1)$.

case -2) Now, if $p \neq q$ and $q = 2$ then $(p, 2)_v = 1, \forall v \neq 2, p$,
$$(p, 2)_2 = (-1)^{\omega(p)} \qquad \text{and} \qquad (p, 2)_p = \left(\frac{2}{p}\right) = (-1)^{\omega(p)}.$$

case -3) Now, if both p and q are different from 2,
$$(p, q)_v = \begin{cases} 1, & \text{if } v \neq 2, p, q, \\ (-1)^{\epsilon(p)\epsilon(q)}, & \text{if } v = 2, \\ \left(\frac{q}{p}\right), & \text{if } v = p, \\ -\left(\frac{p}{q}\right), & \text{if } v = q. \end{cases}$$

We know the quadratic reciprocity law which is,
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\epsilon(p)\epsilon(q)}.$$

Thus,

$$\prod(a,b)_v = \prod(p,q)_v = 1.$$

□

Remark 3.2.2. *The product formula is essentially equivalent to the quadratic reciprocity law. It will come when the set V being replaced by the set of places of the field. This means that when it extends to all the algebraic number fields.*

3.2.2 Existence of rational numbers with given Hilbert symbol

Theorem 3.2.3. *Let $(a_i)_{i\in I}$ be a finite family of elements in $\mathbb{Q}^*$ and let $(\epsilon_{i,v})_{i\in I, v\in V}$ be a finite family of numbers equals to ± 1. There is $x \in \mathbb{Q}^*$ such that $(a_i, x)_v = \epsilon_{i,v}$ for all $i \in I$ and all $v \in V$, it is necessary and sufficient that the following conditions be satisfied:*

1) Almost all $\epsilon_{i,v}$ are equal to 1.

2) For all $i \in I$, we have $\prod_{v\in V} \epsilon_{i,v} = 1$.

3) For all $v \in V$ there exists $x_v \in \mathbb{Q}_v^*$ such that $(a_i, x_v)_v = \epsilon_{i,v}$ for all $i \in I$.

The necessity of first and second condition is follows form previous theorem. For third condition take x_v to be x. To prove sufficiency of above conditions, we need the following three results, then we shall prove this theorem.

Theorem 3.2.4 (Chinese remainder theorem)**.** *Let $a_1, \ldots, a_n$ and $m_1, \ldots, m_n$ be integers with the m_i being pairwise relatively prime. There exists an integer a such that $a \equiv a_i \pmod{m}_i$ for all i.*

Proof. Let's take $M = m_1 \ldots m_n$, and $M_i = M/m_i$. Then, $\gcd(M_i, m_i) = 1$.

$$X \equiv a_1M_1y_1 + \ldots + a_nM_ny_n \pmod{M}.$$

This implies there is $x, y \in \mathbb{Z}$ such that $y_iM_i + b_im_i = 1$.

$$\begin{aligned}
&\Rightarrow M_iy_i \equiv 1 \pmod{m_i} \\
&\Rightarrow\ a_iM_iy_i \equiv a_i \pmod{m_i}, \\
&\Rightarrow\ a_iM_iy_i \equiv 0 \pmod{m_j},\ \text{for } j \neq i, \\
&\Rightarrow\ X \equiv a_i \pmod{m_i},
\end{aligned}$$

and

$$X = \sum_{i=1}^{n} a_iM_iy_i.$$

Now, define map

$$F : \mathbb{Z} \to \mathbb{Z}/M_1\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z} \times \cdots \times \mathbb{Z}/M_n\mathbb{Z}$$

by

$$z \mapsto (z \pmod{M_1}, \ldots, z \pmod{M_n}).$$

Kernel of F is $M_1 m_2 \ldots M_n\mathbb{Z}$. It is easy to see that it is homomorphism, which is injective and surjective.

$$\Rightarrow \mathbb{Z}/M_1M_2\ldots M_n\mathbb{Z} \cong \mathbb{Z}/M_1\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z} \times \cdots \times \mathbb{Z}/M_n\mathbb{Z}$$

□

Theorem 3.2.5 (Approximation theorem)**.** *Let S be the finite subset of V. Then the image of $\mathbb{Q}$ is dense in product $\prod_{v \in S} \mathbb{Q}_v$.*

Proof. This result basically states that for any finite set of places, that is a finite subset S of V. Suppose that $S = \{p_1, p_2, \ldots, p_n, \infty\}$, where all primes are distinct. Our claim is to show that $\mathbb{Q}$ is dense in $\mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_n} \times \mathbb{R}$. Let $x = (x_1, \ldots, x_n, x_\infty)$ be a point of this product and want to show that this point is adherent to $\mathbb{Q}$. Since, all $x_i \in \mathbb{Q}_{p_i}$, we can multiply by suitable integer and make them into from $\mathbb{Z}_{p_i}$ $(i.e.\ x_i \in \mathbb{Z}_{p_i}$, for $1 \leq i \leq n)$. We let ϵ be any positive real number and N be any natural number. By Chinese remainder theorem there exists some $x_0 \in \mathbb{Z}$ such that $\nu_{p_i}(x_0 - x_i) \geq N$ for all i. This follows from the existence of $x_0 \in \mathbb{Z}$ such that $x_0 \equiv x_i \pmod{p_i^N}$. Now an integer $q \geq 2$ is chosen relatively prime to all the p_i. Rational numbers of the form a/q^m with $a \in \mathbb{Z}$ and m some non-negative number are dense among the real numbers. This follows from the divergence of q^m as m goes to infinity. So we find a number $u = a/q^m$ such that,

$$|x_0 - x_\infty + up_1^N \ldots p_n^N| \leq \epsilon.$$

So if we set $x = x_0 + up_1^N \ldots p_n^N$ we have the desired result;

$$|x - x_\infty| \leq \epsilon, \quad \text{and} \quad \nu_{p_i}(x - x_i) \geq N.$$

□

Theorem 3.2.6 (Dirichlet theorem)**.** *If a and m are relatively prime integers greater than 1, there exists infinitely many primes p such that $p \equiv a \pmod{m}$*

Finally, come back to proof of Theorem 3.2.3, tie together these ideas to prove the sufficiency of the conditions.

Proof. Let $(\epsilon_{i,v})$ be a family of numbers satisfying $(1), (2)$, and (3). Via multiplication by square of some integer (recall Hilbert symbol is trivial on squares) we may assume that the a_i are integers. So we let

$$S = \{\infty, 2\} \cup \{\text{ prime factors of } a_i\},$$

$$T = \{v \in V : \exists i \in I \text{ such that } \epsilon_{i,v} = -1\}.$$

Note that both sets above are clearly finite, because there are finitely prime factors in S and also there are finitely many v for $\epsilon_{i,v} = -1$. The argument now splits into two cases.

1) When $S \cap T = \emptyset$, take,

$$a = \prod_{l(\neq\infty)\in T} l \qquad \text{and} \qquad m = 8 \prod_{l(\neq 2,\infty)\in S} l.$$

Since, the intersection of S and T is empty, clearly a and m are relatively prime. By Dirichlet theorem, there is a prime $p \notin S \cup T$ such that $p \equiv a \pmod m$. There are infinitely many such primes, so we can choose one outside of any finite set of places, like $S \cup T$. We want to show that $x = ap$ will have the desired property and satisfy Theorem 3.2.3. $i.e.(a_i, x)_v = \epsilon_{i,v}$ for all $i \in I$ and $v \in V$.

a) If $v \in S, \epsilon_{i,v} = 1$, since $S \cap T = \emptyset$ which implies that $(a_i, x)_v = 1(\because (u, v) = 1)$.

b) If $v = \infty$, it is clear that $(a_i, x) = 1$ because, $x > 0$.

c) If $v = l$, we have $x \equiv a^2 \pmod m$, hence $x \equiv a^2 \pmod 8$ for $l = 2$ and $x \equiv a^2 \pmod l$ for $l \neq 2$.

d) If $v = l$ is not in S, a_i is $l-$adic unit, and $l \neq 2$, we have

$$(a_i, b)_l = \left(\frac{a_i}{l}\right)^{\nu_l(b)}, \quad \forall b \in \mathbb{Q}_l^*.$$

e) If $l \notin T \cup \{p\}$, and x is $l-$adic unit, implies its valuation is zero. Then by above formula, $(a_i, x)_l = 1$ also, $\epsilon_{i,l} = 1$ because $l \in T$.

f) If $l \in T$, and $\nu_l(x) = 1$, by condition (3) of Theorem 3.2.3, there is $x_l \in \mathbb{Q}_l^*$ such that $(a_i, x_l)_l = \epsilon_{i,l}$ for all $i \in I$. Since, one of the $\epsilon_{i,l} = -1(\because l \in T)$, we have $\nu_l(x_l) \equiv 1 \pmod 2$ hence,

$$(a_i, x)_l = \left(\frac{a_i}{l}\right) = (a_i, x_l)_l = \epsilon_{i,l}, \forall i \in I.$$

g) Remaining case is $l = p$, which deduce from using product formula,

$$(a_i, x)_p = \prod_{v\neq p}(a_i, x)_v = \prod_{v\neq p} \epsilon_{i,v} = \epsilon_{i,p}.$$

2) General case,
we know that squares of $\mathbb{Q}_v^*$ is a subgroup of $\mathbb{Q}_v^*$. By Approximation theorem, there is a $x' \in \mathbb{Q}^*$ such that x'/x_v is a square in $\mathbb{Q}_v^*$ for all $v \in S$.

$$i.e.(a_i, x')_v = (a_i, x_v)_v = \epsilon_{i,v} \forall v \in S.$$

Now, if we take $\beta_{i,v} = \epsilon_{i,v}(a_i, x')_v$, such that family $(\beta_{i,v})$ verifies condition $(1), (2)$ and (3) and $\beta_{i,v} = 1$, if $v \in S$. By first case($S \cap T = \emptyset$), there is $y \in \mathbb{Q}^*$ such that $(a_i, y) = \beta_{i,v} \forall i \in I$ and for all $v \in V$. Finally, if we take $x = yx'$, it is clear that x has desired properties.

□

Chapter 4

Quadratic forms

We are start working with quadratic forms over arbitrary commutative ring. If 2 is invertible in a commutative ring R, then quadratic forms are essentially interchangeable with symmetric bilinear forms, but if 2 is not invertible, then there is an important distinction. In this chapter we does not consider the case where ring R is a field $\mathbb{K}$ of characteristic two.

Definition 25 (Bilinear form)**.** *A bilinear form on a vector space V is a bilinear map $V \times V \to \mathbb{K}$, where $\mathbb{K}$ is the field of scalars. In other words, a bilinear form is a function $B : V \times V \to \mathbb{K}$ which is linear in each argument separately,*
- $B(u+v, w) = B(u, w) + B(v, w),$ *for all* $u, v, w \in V,$ *and for all* $\alpha \in \mathbb{K}.$
- $B(u, v+w) = B(u, v) + B(u, w),$ *for all* $u, v, w \in V,$ *and for all* $\alpha \in \mathbb{K}.$
- $B(\alpha u, v) = B(u, \alpha v) = \alpha B(u, v),$ *for all* $u, v \in V,$ *and for all* $\alpha \in \mathbb{K}.$

Definition 26 (Quadratic form)**.** *A quadratic form over a field $\mathbb{K}$ is a homogeneous polynomial of degree 2 in n variables with coefficients in $\mathbb{K}$. In other words, let V be a module over a commutative ring R. A function $Q : V \to R$ is called a quadratic form on V if Q satisfies,*
1) $Q(ax) = a^2Q(x),$ *for* $a \in R, x \in V,$
2) *The function* $(x, y) \mapsto Q(x+y) - Q(x) - Q(y)$ *is bilinear form.*

Such a pair (V, Q) is called a quadratic module. If a commutative ring R is any filed $\mathbb{K}$, then V is vector space over $\mathbb{K}$, and we suppose that its dimension is finite.

Definition 27 (Symmetric bilinear form)**.** *A symmetric bilinear form is bilinear form of V over $\mathbb{K}$ which has property, $B(v, u) = B(u, v)$ for all $u, v \in V$.*

If 2 is invertible in $\mathbb{K}$, and (V, Q) is a quadratic module over $\mathbb{K}$, we write B_Q for the associated symmetric bilinear form on V,

$$B_Q(x, y) = \frac{1}{2}(Q(x+y) - Q(x) - Q(y)).$$

This definition make sense of characteristic different from 2. Conversely, if B is a symmetric bilinear form on a module V over $\mathbb{K}$, we write $Q_B(x) = B(x,x)$. One can see that

$$B(x,x) = \frac{1}{2}(Q(x+x) - Q(x) - Q(x)) = \frac{1}{2}(4Q(x) - 2Q(x)) = Q(x).$$

The map $(x,y) \mapsto B(x,y)$ is symmetric bilinear form on $V \times V$, also called the scalar product associated with Q. If (V_1, Q_1) and (V_2, Q_2) are two quadratic modules, a linear map $T : V_1 \to V_2$ such that $Q_2 \circ T = Q_1$ is called a morphism or metric morphism of (V_1, Q_1) into (V_2, Q_2); then $T(x)T(y) = B(x,y)$, for all $x, y \in V$.

Matrix of quadratic forms- Let V be a vector space over $\mathbb{K}$, and $(e_i), 1 \leq i \leq n$ be basis of V. The matrix of Q with respect to this basis is the matrix $A = (a_{ij})$, where $a_{ij} = B(e_i, e_j)$. It is symmetric. If $x = \sum x_i e_i$ is an element of V, then

$$Q(x) = \sum_{i,j}^{n} a_{ij} x_i x_j,$$

which shows that $Q(x)$ is a quadratic form in n variables ($i.e.\ x_1, \ldots, x_n$). If we change basis such that associated matrix B is invertible. The new matrix A' of Q with respect to new basis is BAB^T, where B^T is transpose of B. Also,

$$\det(A') = \det(A) \cdot \det(B)^2.$$

This shows that $\det(A)$ is determined up to multiplication by an element of $\mathbb{K}^{*2}$. In particular, the square-class of the determinant of A depends only on Q, and not on the choice of basis. This square-class is called the discriminant and it is denoted by disc. Its easy to that either disc$(Q) = 0$ or else, disc$(Q) \in \mathbb{K}^*/\mathbb{K}^{*2}$.

4.1 Orthogonality

Definition 28 (Orthogonal)**.** *Let (v, Q) be a quadratic module over $\mathbb{K}$. We say two elements x, y of V are orthogonal if $B(x,y) = 0$.*

Let (v, Q) be a quadratic module over $\mathbb{K}$ and B be a subset of V, then the set of elements orthogonal to B denoted by $B^{\perp}$. It is vector subspace of V.

Remark 4.1.1. *Let V_1 and V_2 be two vector subspace of V over $\mathbb{K}$, then two subspace V_1 and V_2 are said to be orthogonal if $V_1 \subset V_2^{\perp}$ or equivalently $V_2 \subset V_1^{\perp}$. This means that if $x \in V_1$ and $y \in V_2$ then $B(x,y) = 0$.*

Definition 29 (Radical). *Let (v, Q) be a quadratic module over $\mathbb{K}$. The orthogonal complement of V is $V^{\perp}$ itself called radical of V and its denoted by rad(V).*

Co-dimension of radical is called rank of Q. If $\text{rad}(V) = 0$ then we say, Q is non-degenerate. This is equivalent to saying that the discriminant of Q is nonzero, in which case we view it is an element of the $\mathbb{K}^*/\mathbb{K}^{*2}$.

Definition 30 (Dual space). *Given any finite dimensional vector space V over a field $\mathbb{K}$, the dual space V^* is defined as the set of all linear functionals(maps) $\phi : V \to \mathbb{K}$.*

Basis of dual space called dual basis, and as an important result, which we will be using is that a finite-dimensional vector space V is isomorphic to its double dual V^{**}, where double dual is dual of V^*.
Let V be finite dimensional vector space over $\mathbb{K}$, and U is subspace of V, U^* be a dual of U. Let $\sigma_U : V \to U^*$ be map defined by $\sigma_y(x) = B(x, y)$ (where, $y \in U$ and $x \in V$), associated with each $x \in V$ the linear form. Its obvious that σ_U is homomorphism and kernel is $U^{\perp}$. Now, its is easy to see that Q is non-degenerate if map $\sigma_V : V \to V^*$ forms an isomorphism. By above discussion, we have equivalent condition for non-degeneracy. Q is non-degenerate is equivalent to saying that $\text{disc}(Q) \neq 0$ is equivalent to saying that σ_V is an isomorphism.

Definition 31. *Let $U_1, \ldots, U_n$ be a vector subspace of V. We say V is the orthogonal direct sum of the U_i, if they are pairwise orthogonal and if V is direct sum of them. We denotes,*

$$V = U_1 \widehat{\oplus} \cdots \widehat{\oplus} U_n.$$

If $x \in V$, has for components $x_i \in U_i$ then,

$$Q(x) = Q_1(x_1) + \ldots + Q_n(x_n),$$

where, $Q_i = Q|U_i$ denotes the restriction of Q to U_i. Conversely, if (U_i, Q_i) is a family of quadratic modules, the formula above endows $V = \bigoplus U_i$ with a quadratic form Q, called the direct sum of the Q_i, then $V = U_1 \widehat{\oplus} \cdots \widehat{\oplus} U_n$.

Definition 32 (Supplementary subspace). *Let U_1 and U_2 be two subspaces of the same vector space V. The sum of these subspaces, denoted $U_1 + U_2$, is the set of all the sums $u_1 + u_2$, where $u_1 \in U_1$and $u_2 \in U_2$. If $U_1 \cap U_2 = \{0\}$, the sum is a direct sum and is denoted $U_1 \oplus U_2$. If $U_1 \oplus U_2 = V$, then U_1 and U_2 are supplementary subspaces.*

Proposition 4.1.2. *If V is a vector space and U is a supplementary subspace of rad$(V) = V^{\perp}$, then $V = U \widehat{\oplus} V^{\perp}$.*

Proof. There is nothing to prove, its clear by definition of supplementary subspace and its because U is subspace of V, which is orthogonal to rad(V). □

Proposition 4.1.3. *Suppose (V, Q) is non-degenerate. Then,*

i) All metric morphisms of V into quadratic module (V', Q') are injective.

ii) For all vector subspaces U of V, we have

$$U^{\perp\perp} = U,\ \dim(U) + \dim(U^{\perp}) = \dim(V),\ \textit{rad}(U) = \textit{rad}(U^{\perp}) = U \cap U^{\perp}.$$

The quadratic module U is non-degenerate if and only if $U^{\perp}$ is non-degenerate, in which case $V = U \widehat{\oplus} U^{\perp}$.

iii) If V is the orthogonal direct sum of two subspaces, they are non-degenerate and each of them is orthogonal to each other.

Proof. i) We know that function $T : V \to V'$ is linear such that $Q' \circ T = Q$, then $T(x)T(y) = B(x, y)$. If $T(x) = 0$, we have

$$B(x, y) = T(x)T(y) = 0,\ \text{for all } y \in V;$$

which implies $x = 0$, because (V, Q) is non-degenerate.

ii) Recall map $\sigma_U : V \to U^*$. We also know that kernel is $U^{\perp}$,

$$\dim(V) = \dim(U^{\perp}) + \dim(U^*) = \dim(U) + \dim(U^{\perp}).$$

This shows that U and $U^{\perp\perp}$ have same dimension, since U is contained in $U^{\perp\perp}$ we have $U = U^{\perp\perp}$, rad$(U) = U \cap U^{\perp}$ is clear. If we apply rad$(U) = U \cap U^{\perp}$ to $U^{\perp}$ then rad$(U^{\perp}) = U^{\perp} \cap U$, because $U^{\perp\perp} = U$. Thus, rad(U) =rad$(U^{\perp})$.

iii) If $V = U_1 \widehat{\oplus} U_2$, then rad$(V)$ =rad$(U1)\oplus$rad$(U2)$. Thus rad$(V) = 0$ if and only if the same is true of U_1 and U_2.

□

4.2 Isotropic vectors

Definition 33 (Isotropic)**.** *An isotropic vector in a quadratic module (V, Q) is simply a vector v satisfying $Q(v) = 0$. Such vectors form a quadric hypersurface in V. More generally, a subspace $U \subset V$ is called isotropic if all of its vectors are isotropic.*

Lemma 4.2.1. *Let (V, Q) be a quadratic module and U is a subspace of V,then*

$$U \text{ is isotropic} \iff U \subset U^{\perp} \iff Q|U = 0.$$

Proof. Its clear from definition of isotropic subspace and orthogonal subset $U^{\perp}$ of V. □

Definition 34 (Hyperbolic plane)**.** *A hyperbolic plane is a quadratic module (V, Q) of rank two, which has a basis of isotropic vectors v_1, v_2, satisfying $B_Q(v_1, v_2) \neq 0$.*

Discriminant of matrix with respect to v_1, v_2 is -1, because after multiplying v_2 by $1/v_1v_2$, we can suppose that $B(v_1, v_2) = 1$. Then the matrix of quadratic form with respect to v_1 and v_2 is 2×2 matrix, which opposite diagonal entries are one, that's why discriminant is -1.

Proposition 4.2.2. *Let (V, Q) be a non-degenerate quadratic module and x be an nonzero isotropic element of V. Then there is a subspace U of V which contains x and which is a hyperbolic plane.*

Proof. Since, V is non-degenerate, we can find an element y in V such that $B(x, y) = 1$ or we can make it to one. Then the element $z = 2y - B(y, y)x = 2y - Q(y)x$ is isotropic.

$$Q(z) = 4Q(y) - 4Q(y)B(x, y) + Q(y)^2Q(x) = 4Q(y) - 4Q(y) \cdot 1 + 0 = 0,$$

which implies that z is isotropic. Also,

$$B(x, z) = 2B(y, x) - Q(y)Q(x) = 2(1) = 2 \neq 0.$$

If we take subspace Z which is span of x and z, then Z satisfies both of the conditions. □

Next corollary saying that if we have non-degenerate quadratic module over a field which contains an isotropic element then quadratic form with respect to V represents all elements of field.

Corollary 4.2.3. *If (V, Q) is non-degenerate quadratic module over $\mathbb{K}$ and contains a nonzero isotropic element x, then one has $Q(V) = \mathbb{K}$.*

Proof. It is suffices to give proof when V is a hyperbolic plane with basis x, y, both isotropic and $B(x, y) = 1$. Now, if $a \in \mathbb{K}$ then

$$Q\left(x + \frac{a}{2}y\right) = Q(x) + a \cdot B(x, y) + \frac{a^2}{4}Q(y) = a.$$

□

4.3 Orthogonal basis

A basis $(e_1, e_2, \ldots, e_n)$ of a quadratic module (V, Q) is called orthogonal if its elements are pairwise orthogonal, which means, if $V = \mathbb{K}e_1 \widehat{\oplus} \cdots \widehat{\oplus} \mathbb{K}e_n$. If we see this as matrix of quadratic form Q with respect to above basis then we get diagonal matrix or we can say that the matrix with respect to orthogonal basis is diagonal. If $x = \sum x_i e_i$, then quadratic form $Q(x_1, \ldots, x_n) = a_1 x_1^2 + \ldots + a_2 x_n^2$ over $\mathbb{K}^n$.

Theorem 4.3.1. *Every quadratic module (V, Q) has an orthogonal basis.*

Proof. We will give proof by induction on $\dim(V)$, the theorem being trivial if dimension is zero. If V is itself isotropic, every element of V is orthogonal to every other element of V. Hence, all bases of V are orthogonal. Otherwise, choose an element $e_1 \in V$, with $Q(e_1) \neq 0$. Let $H = (e_1\mathbb{K})^\perp$, it is hyperplane and since $e_1 \notin H$, it is clear that $V = \mathbb{K}e_1 \widehat{\oplus} H$. By induction on dimension of H, we may find an orthogonal basis of H, say $e_2, \ldots, e_n$, yielding an orthogonal basis $e_1, \ldots, e_n$ of V. □

Definition 35 (Contiguous bases). *Two orthogonal bases $e = (e_1, \ldots, e_n)$ and $f = (f_1, \ldots, f_n)$ of V are said to be contiguous if there is i and j such that $e_i = f_j$, or if they have an element in common.*

Lemma 4.3.2. *Let (V, Q) be a non-degenerate quadratic module of dimension ≥ 3, and let $e = (e_1, \ldots, e_n)$ and $e' = (e'_1, \ldots, e'_n)$ be two orthogonal bases of V. Then there is $x \in \mathbb{K}$ such that $e_x = e'_1 + xe'_2$ is anisotropic and generates with e_1 a non-degenerate plane.*

Theorem 4.3.3. *Let (V, Q) be a non-degenerate quadratic module of dimension ≥ 3, and let $e = (e_1, \ldots, e_n)$ and $e' = (e'_1, \ldots, e'_n)$ be two orthogonal bases of V. Then there exists a finite sequence $e^{(0)}, \ldots, e^{(m)}$ of orthogonal bases of V such that $e^{(0)} = e, e' = e^{(m)}$ and $e^{(i)}$ is contiguous with $e^{(i+1)}$ with $0 \leq i \leq m - 1$.*

Proof. To prove this, we separate proof in three cases.

i) $Q(e_1)Q(e'_1) - B(e_1, e'_1)^2 \neq 0$
We can find chain for two e and e' such that $P = \mathbb{K}e_1 \widehat{\oplus} \mathbb{K}e'_1$, with $Q|_P$ is non-degenerate. Then there is ϵ and ϵ' such that $P = \mathbb{K}e_1 \widehat{\oplus} \mathbb{K}\epsilon = \mathbb{K}\epsilon' \widehat{\oplus} \mathbb{K}e'_1$. Now, let $(e''_3, \ldots, e''_n)$ be orthogonal basis of $P^\perp$, then $V = P \widehat{\oplus} P^\perp$, hence it is non-degenerate.

$$e \to (e_1, \epsilon, e''_3, \ldots, e''_n) \to (e'_1, \epsilon', e''_3, \ldots, e''_n) \to e'.$$

We are done with this case.

ii) $Q(e_1)Q(e'_2) - B(e_1, e'_2)^2 \neq 0$
Same proof works by replacing e'_1 by e'_2.

iii) $Q(e_1)Q(e_i') - B(e_1, e_i') = 0$ for $i = 1, 2$. In particular, $\mathbb{K}e_1 \oplus \mathbb{K}e_1'$ is degenerate, and $\mathbb{K}e_1 \oplus \mathbb{K}e_2'$ is degenerate, but in this case, the previous Lemma 4.3.2 implies that there exists $x \in \mathbb{K}$ such that $e_x' = e_1' + xe_2'$ generates a non-degenerate plane with e_1, and is anisotropic. Indeed, to have e_x' be anisotropic, we must have,

$$Q(e_x') = Q(e_1') + x^2 Q(e_2') \neq 0 \text{ since } e_1' \perp e_2'.$$

Thus as long as $x^2 \neq -Q(e_1')/Q(e_2')$, this will be satisfied. For e_1 and e_x' to generate a non-degenerate plane, we must have;
$0 \neq Q(e_1)Q(e_x') - B(e_1, e_x')^2$
$= Q(e_1)Q(e_1') + x^2 Q(e_1)Q(e_2') - (B(e_1, e_1') + xB(e_1, e_2'))^2$
$= Q(e_1)Q(e_1') + x^2 Q(e_1)Q(e_2') - B(e_1, e_1')^2 - 2xB(e_1, e_1')B(e_1, e_2') - x^2 B(e_1, e_2')^2$
$= Q(e_1)Q(e_1') + x^2 Q(e_1)Q(e_2')Q(e_1)Q(e_1') - 2xB(e_1, e_1')B(e_1, e_2') -$
$x^2 Q(e_1)Q(e_2')$
$= -2xB(e_1, e_1')B(e_1, e_2')$.
Non-degeneracy, together with the fact that $B(e_1, e_1')^2 = Q(e_1)Q(e_1')$ and $B(e_1, e_2')^2 = Q(e_1)Q(e_2')$ implies that for $x \neq 0$, the above condition is satisfied. The existence of e_x' such that e_x' is non-degenerate, and with e_1 it generates a non-degenerate plane, follows from finding $x \in \mathbb{K}$ with,

$$0 \neq x, \quad \text{and} \quad x^2 \neq Q(e_1')/Q(e_2').$$

This eliminates at most three values of x. We dont consider $\mathbb{K} = \mathbb{F}_2$, because we assume $\text{char}(\mathbb{K}) \neq 2$. In $\mathbb{F}_3$, all squares are 0 or 1, and the condition $Q(e_1)Q(e_1') = B(e_1, e_1')^2$ and $Q(e_1)Q(e_2') = B(e_1, e_2')^2$ implies that $Q(e_1')/Q(e_2') = 1$. Thus, choosing $x^2 \neq 1$ does not place any condition on x. Such an x exists. Now, in order to make the transition from e to e', we use the intermediate basis e_x' given by, $e_x' = (e_x', e_2', e_3', \dots, e_n')$. This basis is contiguous to e'. By the previous case, we can find a chain linking e to e_x'.

□

4.4 Witt's theorem

In this section, we consider metric morphisms between quadratic modules and when they can be extended. Specifically, given two non-degenerate quadratic modules (V_1, Q_1) and (V_2, Q_2), an injective morphism $s : U \to V_2$ between $U \subset V_1$, a submodule, and V_2 which preserves the associated bilinear form, we try to extend s to all of V_1. An extension of s is a morphism from a larger space, containing U as a subspace, which is equal to s when restricted to U. Our main result is Witt's theorem which says that such an extension exists if V_1 and V_2 are isomorphic.

Lemma 4.4.1. *If U is degenerate, we can extend s to an injective metric morphism $s_1 : U_1 \to V_2$, where U_1 contains U as hyperplane.*

Proof. Since U is degenerate, we can choose a nonzero $x \in \text{rad}(U)$. Furthermore, since V is non-degenerate we can find a $y \in V$ such that $l_1(x) := [\sigma_y](x) = 1(recall[\sigma_y](u) = B(y,u))$. We can also assume that y is isotropic (if not replace y by $y - \frac{1}{2}Q_1(y)x$, which is clearly isotropic). We then set $U_1 = U \oplus \mathbb{K}y$. Let $U' = s(U)$. Since s is injective we can form a linear functional l_2 on U' by $l_2 = l_1(y) \circ s^{-1}$. As we have seen, V_2 being non-degenerate implies that there exists y_2 such that $l_2 = \sigma_{Q_2}(y_2)$. Thus if we define the map $s_1 : U_1 \to V_2$ by letting s_1 equal s on U and $s_1(y) = y_2$ and extend linearly, then s_1 is a metric morphism. □

Theorem 4.4.2 (Witt's theorem)**.** *If (V_1, Q_1) and (V_2, Q_2) are isomorphic and non-degenerate, every injective metric morphism $s : U \to V'$ of subspace U of V can be extended to V onto V'.*

Proof. We construct our extension inductively on the dimension of U. If U is degenerate, we can apply the above Lemma 4.4.1 repeatedly until we arrive at a non-degenerate submodule, thus we can make the simplifying assumption that U is non-degenerate. Furthermore, since V_1 and V_2 are isomorphic, we can assume that $V = V_1 = V_2$. $\dim U = 1$; Since U is non-degenerate and one-dimensional, it is generated by a non-isotropic element x. Let $y = s(x)$, then we have $Q(x) = Q(y)$ and we can choose an $\epsilon = \pm 1$ such that $x + \epsilon y$ is not isotropic; if not we would have:

$$Q(x+y) = 0$$
$$Q(x-y) = 0$$

expanding the left hand side:

$$B(x,x) + B(x,y) + B(y,x) + B(y,y) = 0$$
$$B(x,x)B(x,y)B(y,x) + B(y,y) = 0$$

Since $B(x,x) = B(y,y)$ and $B(x,y) = B(y,x)$ we have:

$$2B(x,x) + 2B(x,y) = 0$$
$$2B(x,x) - 2B(x,y) = 0$$

which implies that $Q(x) = 0$. Given such an ϵ, we let H be the orthogonal complement of $z = x + \epsilon y$; we have $V = \mathbb{K}z \oplus H$. Define σ to be the automorphism of V which is the identity on H and which sends z to $-z$. Thus,

$$\sigma(x + \epsilon y) = -x - \epsilon y$$

$$\sigma(x - \epsilon y) = x - \epsilon y$$

since $x - \epsilon y \in H$ implying $\sigma(x) = -\epsilon y$, thus $-\epsilon\sigma$ extends s. If $\dim U > 1$: We can decompose U as $U_1 \widehat{\oplus} U_2$ both not zero; restricting s to U_1 and extending by induction we get an automorphism, σ_1, of V which extends s when restricted to U_1. By substituting s with $\sigma_1^{-1} \circ s$ we can suppose s is the identity on U_1. Since s is the identity on U_1 and injective we have that U_2 is contained in the orthogonal complement of U_1, $U^{\perp}$, and thus it suffices to extend $s|_{U_2}$ to a $\sigma_2 : U_1^{\perp} \to U_1^{\perp}$ which we can do by the induction hypothesis. Thus our desired extension is σ which is σ_2 on $U_1^{\perp}$ and $\sigma_1^{-1} \circ s$ on U_1. □

As an application of above theorem, we see that isomorphic subspaces of a non-degenerate quadratic module have isomorphic orthogonal complements.

Corollary 4.4.3. *Two isomorphic subspaces of a non-degenerate quadratic module have isomorphic orthogonal complements.*

Proof. Essentially, if we have a non-degenerate quadratic module (V, Q) with subspaces U_1 and U_2 such that $U_1 \cong U_2$ then we extend the isomorphisms of the subspaces to an automorphism of V, since $V \cong U_1 \widehat{\oplus} U_1^{\perp} \cong U_2 \widehat{\oplus} U_2^{\perp}$ when we restrict the automorphism to the orthogonal complements and get $U_1^{\perp} \cong U_2^{\perp}$ □

4.5 Equivalence of quadratic forms

Let $X \in \mathbb{K}^n$ we consider a quadratic form

$$f(X) = \sum_{i=1}^{n} a_{ii} X_i^2 + 2 \sum_{i>j} a_{ij} X_i X_j$$

in n variables over $\mathbb{K}$. Set $a_{ij} = a_{ji}$ for $i > j$, the matrix $A = (a_{ij})$ is symmetric and the pair $(\mathbb{K}^n, A)$ is a quadratic module, associated to f.

Definition 36. *Two quadratic forms f and f', in n variables, are equivalent, if there is a an invertible matrix M such that $f(MX) = f'(X)$ or A and B are matrix of f and f',if there is an invertible matrix C such that $B = CAC^T$.*

Definition 37. *Let $f(X_1, \ldots, X_n)$ and $g(X_1, \ldots, X_m)$ be two quadratic forms. The translation of a one quadratic form by another, denoted $f + g$, is defined to be the quadratic form given by;*

$$f + g = f(X_1, \ldots, X_n) + g(X_{n+1}, \ldots, X_{n+m}).$$

In terms of the associated modules, this operation corresponds to the orthogonal sum. We similarly define $f - g$ for $f + (-g)$. We now translate several of our definitions and theorems in terms of translations. First notice that our hyperbolic plane has associated form $f(X) = X_1X_2 \cong X_2^2 - X_2^2$ which is clearly a translation of two one variable forms.

Definition 38. *Let Q be a quadratic form over $\mathbb{K}$. We say that a quadratic form represents an element $a \in \mathbb{K}$ if there exists a vector $x \in \mathbb{K}^n$ such that $f(x) = a$.*

Remark 4.5.1. *f represents zero if and only if corresponding quadratic module contains nonzero isotropic element.*

Proposition 4.5.2. *If f_1 represents zero and is non-degenerate, then $f_1 \sim f_2 + g$ where f_2 is hyperbolic. Moreover, f represents all elements of $\mathbb{K}$.*

Proof. If $0 \neq x \in V$ is isotropic of non-degenerate, which implies there is subspace U of V which contains x and which is hyperbolic plane. Now, by finding orthogonal complement $U^\perp$ of U, that is f_2 with respect to U is hyperbolic and g with respect to $U^\perp$. Thus, it is clear that $f_1 \sim f_2 + g$. We know that if we have non-degenerate and contains an isotropic element then $Q(V) = \mathbb{K}$ □

Following corollary shows importance of above theorem.

Corollary 4.5.3. *Let $g = g(X_1, \ldots, X_n)$ be a non-degenerate quadratic form and let $a \in \mathbb{K}^*$. Then the following are equivalent.*

1) *g represents a.*

2) *One has $g \sim h + aZ^2$ where h is a form in $n-1$ variables.*

3) *The form $f = g - aZ^2$ represents 0.*

Proof. $1) \Rightarrow 2)$ If g generates a, quadratic module V corresponding to g contains an elements x such that $B(x, x) = a$. Then, find orthogonal complement of x, let say it is H, then $V = H \widehat{\oplus} \mathbb{K}x$. Finally, $g \sim h + aZ^2$, where h is form denotes the quadratic form attached to a basis of H.
$2) \Rightarrow 1)$ $g \sim h + aZ^2$, h is in $n-1$ variables then,
$g \sim h(0, 0, \ldots, 0) + aZ^2 = h(0, 0, \ldots, 0) + a(1) = a$. Thus, g represents a.
$2) \Rightarrow 3)$ We know that $g \sim h + aZ^2$ represents a, because g represents a with $(y_1, \ldots, y_n)$, then the form $f = g(y_1, \ldots, y_n) - a(1) = a - a = 0$ represents zero.
$3) \Rightarrow 1)$ f has non-trivial zero $(x_1, \ldots, x_{n-1}, z)$ then $z = 0$ when g represents zero. Thus, it represents a also. Now, if $z \neq 0$ then,

$$f(x_1/z, x_2/z, \ldots, x_{n-1}/z, 1) = g(x_1/z, x_2/z, \ldots, x_{n-1}/z) - a = 0,$$

thus, g represents a. □

Corollary 4.5.4. *Let g and h be two non-degenerate forms of rank greater or equal to 1, and $f = g - h$ then the following are equivalent.*

1) f represents zero.

2) There is $a \in \mathbb{K}^*$, which is represented by g and h.

3) There is $a \in \mathbb{K}^*$ such that $g - aZ^2$ and $h - aZ^2$ represents zero.

Proof. $1) \Rightarrow 2)$ Nontrivial zero of f can be written as (x, y) such that $g(x) = h(y)$. If $a = g(x) = h(y) \neq 0$ implies (2) is done. If $a = 0$, then $g(x) = 0$, also g represents all elements of $\mathbb{K}$. g also represents any nonzero values taken by h.
$2) \Rightarrow 1)$ This is trivial, because both g and h represents a, but $f = g - h$ then it is clear that f represents zero.
$2) \iff 3)$ Equivalence of (2) and (3) is follows from previous corollary. □

Next theorem translates into the classical decomposition of quadratic forms.

Theorem 4.5.5. *Let f be a quadratic form with n variables. Then there is $a_1, \ldots, a_n \in \mathbb{K}$ such that $f \sim a_1X_1^2 + \ldots + a_nX_n^2$.*

The rank of f is the number of indices i such that $a_i \neq 0$. It is equal to n if and only if the discriminant $a_1, \ldots, a_n$ of f is $\neq 0$, equivalently to saying if f is non-degenerate. Finally, corollary to Witt's theorem gives cancellation theorem.

Theorem 4.5.6 (Cancellation theorem). *Let $f = g + h$ and $f' = g' + h'$ be two non-degenerate quadratic forms. If $f \sim f'$ and $g \sim g'$ then $h \sim h'$.*

Corollary 4.5.7. *If f is non-degenerate, then*

$$f \sim g_1 + \ldots + g_n + h,$$

where, $g_1, \ldots, g_n$ are hyperbolic and h does not represents zero. This decomposition is unique up to equivalence.

Proof. By Proposition 4.5.2, $f \sim g_1 + h_1$ with both non-degenerate, we can repeat and get up to n. For uniqueness, $f \sim g_1 + \ldots + g_n + h \sim g'_1 + \ldots + g'_k + h'$. Then by cancellation theorem $h \sim h'$ and $n = k$ and h is called an isotropic part of f. □

4.6 Quadratic forms over $\mathbb{F}_q$

In this section we completely classify the quadratic forms over the finite fields of characteristic different from two. We let p be prime $\neq 2$ and $q = p^f$. Let $\mathbb{F}_q$ be the field with q elements.

Proposition 4.6.1. *A quadratic form over $\mathbb{F}_q$ of rank ≥ 2 (respectively of rank ≥ 3) represents all elements of $\mathbb{F}_q^*$ (respectively of $\mathbb{F}_q$).*

Proof. In view of corollary 4.5.3 it is sufficient to prove that all quadratic forms in 3 variables represent zero and this we have already proved in Chevalley-Warning Theorem 1.2.4. We can prove it in other way also, One has to show that , if $a, b \in \mathbb{F}_q$ are not zero, the equation

$$ax^2 + by^2 = c$$

has a solution. Let $A = \{m \in \mathbb{F}_q : m = ax^2\}$ and $B = \{z \in \mathbb{F}_q : z = c - by^2\}$ where, $x, y \in \mathbb{F}_q$. One can see that A and B both have each $(q+1)/2$ elements; thus $A \cap B \neq \emptyset$, then it is clear that one can get solution of equation $ax^2 + by^2 = c$. □

Recall that group $\mathbb{F}_q^*/\mathbb{F}_q^{*2}$ has two elements. Let a denote an element of $\mathbb{F}_q^*$ which is not a square.

Proposition 4.6.2. *Every non-degenerate quadratic form of rank n over $\mathbb{F}_q$ is equivalent to*

$$X_1^2 + \ldots + X_n^2$$

or

$$X_1^2 + \ldots + X_{n-1}^2 + aX_n^2,$$

depending on whether its discriminant is a square or not.

Proof. If $n = 1$ this is clear. If $n \geq 2$, Proposition 4.6.1 shows that the form f represents 1. Thus, it is equivalent to $X_1^2 + g$ where g is form in $n - 1$ and then by inductive hypothesis on g. □

Corollary 4.6.3. *For two quadratic forms over $\mathbb{F}_q$ to be equivalent it is necessary and sufficient that they have same rank and same discriminant.*

Finally, we can see that quadratic forms over $\mathbb{F}_q$ are completely determined (up to equivalence) by their rank and their discriminant.

Chapter 5

Quadratic forms over $\mathbb{Q}_p$

Conventions for the chapter include that p is a prime number, $\mathbb{K}$ is the p-adic number field and quadratic modules and forms over $\mathbb{K}$ are assumed to be non-degenerate.

5.1 Invariants

Here we let (V, Q) be a quadratic module of rank n and $d(Q) \in \mathbb{K}^*/\mathbb{K}^{*2}$ its discriminant. If $e = (e_1, \ldots, e_n)$ is an orthogonal basis of V and we set $a_i = B(e_i, e_i) = Q(e_i)$, then

$$d(Q) = \prod_{i}^{n} a_i.$$

Recall for $a, b \in \mathbb{K}^*$, the Hilbert symbol $(a, b) \in \{\pm 1\}$ is already defined. We define

$$\epsilon(e) := \prod_{i<j} (a_i, a_j) \in \{\pm 1\}.$$

We shall show that this $\epsilon(e)$ is an invariant of (V, Q), that is, it does not depend on the choice of orthogonal basis e.

Theorem 5.1.1. *The number $\epsilon(e)$ does not depend on the choice of the orthogonal basis e.*

Proof. We prove this theorem through induction on the rank of V. If $n = 1$ then $\epsilon(e) = 1$. If $n = 2$ then we have that

$$\epsilon(e) = 1 \iff Z^2 a_1 X^2 - a_2 Y^2 \text{ represents } 0 \iff a_1 X^2 + a_2 Y^2 \text{ represents } 1$$

Then $v \in V$ such that $Q(v) = 1$ and such a v is independent of any choice of basis. For $n \geq 3$, induction is used. By Theorem 4.3.3 and transitivity it is enough to show that $\epsilon(e) = \epsilon(e')$ when e and

e' are contiguous. Moreover the symmetry of the Hilbert symbol implies that we can assume that $e' = (e'_1, \ldots, e'_n)$ with $e_1 = e'_1$. So with $a'_i = Q(e'_i)$ it follows that $a_1 = a'_1$. We then write

$$\begin{aligned}\epsilon(e) &= \prod_{k=2}^{n}(a_1, a_k) \prod_{2 \leq i \leq j}(a_i, a_j)\\ &= (a_1, a_2 \ldots a_n) \prod_{2 \leq i \leq j}(a_i, a_j)\\ &= (a_1, d(Q)a_1) \prod_{2 \leq i \leq j}(a_i, a_j).\end{aligned}$$

Similarly we have $\epsilon(e') = (a_1, d(Q)a_1) \prod_{2 \leq i \leq j}(a'_i, a'_j)$ and so the proof is done by induction. So given a quadratic form we immediately have two invariants, the discriminant and the epsilon sign invariant. By inductive hypothesis applied to orthogonal complement of e_1 shows that

$$\prod_{2 \leq i \leq j}(a_i, a_j) = \prod_{2 \leq i \leq j}(a'_i, a'_j),$$

from the desired result follows. □

5.2 Representation of an element

Let $a \in \mathbb{K}^*/\mathbb{K}^{*^2}$, $\epsilon = \pm 1$, then define

$$H_a^\epsilon \;=\; \{x \in \mathbb{K}^*/\mathbb{K}^{*^2} | (x, a) = \epsilon\}.$$

Lemma 5.2.1. *Representation of an element of* $\mathbb{K}$ *by* $\mathbb{Q}_f$

1) Let H_a^ϵ *be defined as above.*
If $a = 1$, $\#(H_a^1) = 2^r$ *and* $Ha^{-1} = \phi$
If $a \neq 1$, $\#(H_a^\epsilon) = 2^{r-1}$

2) Let $a, a' \in \mathbb{K}^*/\mathbb{K}^{*^2}$, $\epsilon, \epsilon' = \pm 1$, $H_a^\epsilon, H_{a'}^{\epsilon'} \neq \phi$, $H_a^\epsilon \cap H_{a'}^{\epsilon'} = \phi$. *It is necessary and sufficient condition that* $a = a'$ *and* $\epsilon = -\epsilon'$

Proof. 1) $a = 1$, then it is a square. This implies $H_a^1 = 2^r$, thus, $H_a^{-1} = \phi$.
If $a \neq 1$, Define $\phi : \mathbb{K}^*/\mathbb{K}^{*^2} \twoheadrightarrow \pm 1$ by $b \mapsto (a, b)$. $\ker(\phi) = H_a^k$, which is a hyperplane with cardinality 2^{r-1}. Thus, $\#(H_a^{-1}) = 2^{r-1}$.
2) $H_a^\epsilon \cap H_{a'}^{\epsilon'} = \emptyset$
$\#(H_a^\epsilon) = \#H_{'a}^{\epsilon'} = 2^{r-1}$, because $2^{r-1} + 2^{r-1} = 2^r$. This implies $H_a^1 = H_{a'}^1$ then $(x, a) = (x, a')$ for all $x \in \mathbb{K}^*/\mathbb{K}^{*^2}$. □

Theorem 5.2.2. *For f to represent zero it is necessary and sufficient that*

1. $n = 2$ *and* $d = -1 \in \mathbb{K}^*/\mathbb{K}^{*2}$
2. $n = 3$ *and* $(-1, -d) = \epsilon$
3. $n = 4$ *and either* $d \neq 1$ *and* $(-1, -1) = \epsilon$
4. $n \geq 5$*, all forms in at least* 5 *variables represents zero.*

Before proving this theorem, let us indicate a consequence of it. Let $a \in \mathbb{K}^*/\mathbb{K}^{*2}$ and $f_a = f - aZ^2$. We already know that if f represent zero if and only if it represent a. Other hand,

$$d(f_a) = -ad, \quad \epsilon(f_a) = (-a, d)\epsilon.$$

as one can check right away.

Corollary 5.2.3. *Let* $a \in \mathbb{K}^*/\mathbb{K}^{*2}$*. Quadratic form f represent a it is necessary and sufficient that :*

1. $n = 1$ *and* $a = d$
2. $n = 2$ *and* $(a, -d) = \epsilon$*,*
3. $n = 3$ *either* $a \neq d$ *or* $a = -d$ *and* $(-1, -d) = \epsilon$*,*
4. $n \geq 4$.

Note that, in this statement as in above theorem, a and d are viewed as elements of $\mathbb{K}^*/\mathbb{K}^{*2}$, the inequality $a \neq -d$ means that a is not equal to the product of $-d$ by a square. Now, go back to prove above theorem.

Proof. 1. $n = 2$:
The form represents zero if and only if $-a_1/a_2$ is a square, but
$-a_1/a_2 = -a_1a_2 = -d \in \mathbb{K}^*/\mathbb{K}^{*2}$. Hence this means that $d = -1$.

2. $n = 3$:
The form f represents zero if and only if the form

$$-a_3 f \sim -a - 3a_1X_1^2 - a_3a_2X_2^2 - X_3^2$$

represents zero. Now by very definition of the Hilbert symbol, this last form represents zero if and only if we have

$$(-a_3a_1, -a_3a_2) = 1$$

. because,

$$(-1,1)(-1,-a_1)(-1,-a_2)(a_3,a_3)(a_1,a_2)(a_1,a_3)(a_2,a_3) = 1$$

and,

$$(-1,1)(-1,a_1a_2a_3)(a_1,a_2)(a_1,a_3)(a_2,a_3) = 1$$

3. $n = 4$:

   From Corollary 4.5.4, f represents zero if and only if there exists an element $x \in \mathbb{K}^*/\mathbb{K}^{*2}$, which is represented by two forms.

   $$a_1X_1^2 + a_2X_2^2 \text{ and } \; - a_3X_3^2 - a_4X_4^2$$

   By above corollary, such as x characterized by the conditions,

   $$(x, -a_1a_2) = (a_1, a_2) \text{ and } \; (x, -a_3a_4) = -a_3, -a_4).$$

   Let A be the subset of $\mathbb{K}^*/\mathbb{K}^{*2}$ defined by the first condition, and let B be the subset defined by the second. f does not represent zero, it is necessary and sufficient the $A \cap B = \emptyset$ Now, A and B are clearly non-empty, and the relation $A \cap B = \emptyset$ is thus equivalent to

   $$a_1a_2 = a_3a_4 \;\text{ and }\; (a_1, a_2) = -(-a_3, -a-4)$$

   The first condition means that $d = 1$. If it is fulfilled one has,

   $$\epsilon = (a_1, a_2)(a_3, a_4)(a_3a_4, a_3a_4),$$

   by using the relation$(x, x) = (-1, x)$, we get,

   $$\epsilon = (a_1, a_2)(a_3, a_4)(-1, a_3a_4),$$

   $$= (a_1, a_2)(-a_3, a_4)(-1, 1),$$

   Hence, second condition can be written $\epsilon = -(-1, -1)$, form which the result follows.

4. $n \geq 5$:

   It is sufficient to treat that $n = 5$, by using 3^{rd} condition of above corollary, we see that form of rank 2 reprsents at least 2^{r-1} elements if $\mathbb{K}^*/\mathbb{K}^{*2}$ and the same is true for the form of rank ≥ 2. Since, $2^{r-1} \geq 2$ represents at least one element $a \in \mathbb{K}^*/\mathbb{K}^{*2}$ distinct form d. Then one has,

   $$f \sim aX^2 + g,$$

   where g is form of rank 4. The discriminant of g is equal to d/a, it is thus different from 1, and form 3, the form represents zero. The same is then true for f and the proof of theorem is complete.

□

5.3 Classification

Theorem 5.3.1. *Two quadratic forms over $\mathbb{K}$ are equivalent if and only if they have same rank, same discriminant, and same invariant.*

Proof. That two equivalent forms have same invariants follows from the definitions. The converse part is proved by induction on the rank n of two forms f and g considered. The case $n = 0$ is trivial. If we let f and g be two quadratic forms of rank n, discriminant d and invariant ϵ, both f and g represent the exact same elements from $\mathbb{K}^*/\mathbb{K}^{*^2}$ and so we can find some a that is represented by both which implies that $f \sim aZ^2 + f'$ and $g \sim aZ^2 + g'$ with f', g' quadratic forms of rank $n-1$,

$$d(f') = ad(f) = ad(g) = d(g')$$

and

$$\epsilon(f) = \epsilon(f)(a, d(f')) = \epsilon(g)(a, d(g')) = \epsilon(g'),$$

which shows that f' and g' have same invariants. This implies $f' \sim g'$, thus $f \sim g$. □

Proposition 5.3.2. *Let $n \geq 1,\ d \in \mathbb{K}^*/\mathbb{K}^{*^2}$ and $\epsilon = \pm 1$. There exists a quadratic form f of rank n such that $d(f) = d$ and $\epsilon(f) = \epsilon$, it is necessary and sufficient that $n = 1, \epsilon = 1$, or $n = 2, d \neq 1$ or $n = 2, \epsilon$ or $n \geq 3$.*

Proof. Case $n = 1$ is trivial. If $n = 2$ one has $f \sim aX^2 + bY^2$ and,

$$\text{if} \quad d(f) = -1, \text{ then } \epsilon(f) = (a, b) = (a, -ab) = 1;$$

thus we can not have simultaneously $d(f) = -1$ and $\epsilon(f) = -1$. Conversely, if $d = -1, \epsilon = 1$, we take $f = X^2 - Y^2$; if $d \neq -1$, there exists $a \in \mathbb{K}$, such that $(a, -d) = \epsilon$ and $f = aX^2 + adY^2$. If $n = 3$ we choose $a \in \mathbb{K}^*/\mathbb{K}^{*^2}$ distinct from $-d$, y what we have just seen, there exists a form g of rank 2 such that $d(g) = ad, \epsilon(g) = \epsilon(a, -d)$, then the form $aZ^2 + g$ works. The case $n \geq 4$ is reduced to the case $n = 3$ by taking $f = g(X_1, X_2, X_3) + X_4^2 + \ldots X_n^2$ where g has required invariants. □

We let f be a quadratic form of rank n over the real numbers. We know f is equivalent to $X_1^2 + \ldots + X_r^2 - Y_1^2 - \ldots - Y_s^2$ where r, s are two non-negative integers whose sum is n. The pair r, s depend only on f and is called the signature of the form f. The form f is positive or negative definite if $s = 0$ or $r = 0$ and otherwise f is indefinite (f represents 0 in that case and only in that case). The invariant $\epsilon(f)$ is defined as before and due to $(-1, -1) = -1$ we have the following; $\epsilon(f) = (-1)^{s(s-1)/2}$ and $d(f) = (-1)^s$. So if n is less than or equal to three, these two invariants determine f up to equivalence!

Chapter 6

Quadratic forms over $\mathbb{Q}$

In this chapter, all quadratic forms have coefficients in $\mathbb{Q}$, and are non-degenerate. The quadratic form $Q(X_1, \dots, X_n) = a_1 X_1^2 + \dots + a_n X_n^2$. Every quadratic module has an orthogonal basis, and thus is equivalent to $a_1 X_1^2 + \dots + a_n X_n^2$. We always assume that $0 \neq a_i \in \mathbb{Q}$ for all $1 \leq i \leq n$.

6.1 Invariants

Recall that V is the set of places of $\mathbb{Q}$, and $\infty \in V$ is the real place, with $\mathbb{Q}_\infty = \mathbb{R}$. Two invariants of a non-degenerate quadratic form, over any field $\mathbb{K}$ of characteristic not equal to 2, are the discriminant $d = \prod_{i=1}^n a_i$. It is interpreted in $\mathbb{K}^*/\mathbb{K}^{*2}$, the ϵ-invariant is defined by

$$\epsilon = \prod_{1 \leq i \leq j \leq n} (a_i, a_j) \in \{\pm 1\},$$

where (a_i, a_j) denotes the Hilbert symbol. If f is a quadratic form over $\mathbb{Q}$, we write $\epsilon_v = \pm 1$ for the invariant of f, viewed as a quadratic form over $\mathbb{Q}_v$, and we write $d_v \in \mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$ for the discriminant of f viewed as a quadratic form over $\mathbb{Q}_v$. Product formula of Hilbert symbol gives one,

$$i.e. \prod_{v \in V} \epsilon_v(f) = 1.$$

We write r, s for the number of ones and negative ones, as invariants of f over $\mathbb{R}$.

6.2 Hasse-Minkowski theorem

Next theorem says that f has a global zero if and only f has everywhere a local zero.

Theorem 6.2.1 (Hasse-Minkowski)**.** *Let f be a quadratic form over $\mathbb{Q}$. f represents zero, it is necessary and sufficient that, for all $v \in V$, the form f_v represent zero.*

Proof. We write quadratic form,

$$f = a_1X_1^2 + \ldots + a_nX_n^2,\ a_i \in \mathbb{Q}^*.$$

Replacing f by a_1f, one can suppose that $a_1 = 1$. We consider separately the cases $n = 2, 3, 4$ and ≥ 5.

- $n = 2$:
  Suppose that $f = X^2 + aY^2$ over $\mathbb{Q}$ and f represents zero over $\mathbb{Q}_p$, for every prime p. Since f represents zero over $\mathbb{R}$, we have $a < 0$. Thus it suffices to consider $f = X^2 - aY^2$ with $0 < a \in \mathbb{Q}$. This represents zero if and only if $a \in \mathbb{Q}^{*^2}$. Since f represents 0 over $\mathbb{Q}_p$, for every p, we have $a \in \mathbb{Q}_p^{*^2}$. Thus, $\nu_p(a)$ is even for all p; recall that $\nu_p(a)$ is the exponent of p in the prime factorization of a. Since a is positive, we see that $a = \prod_p p^{\nu_p(a)}$, for even integers $\nu_p(a)$. Hence, $a \in \mathbb{Q}^{*^2}$ as desired.

- $n = 3$:
  we have $f = X_1^2 - aX_2 - bX_3^2$. We can assume that a and b are square free integers, which means $\nu_p(a), \nu_p(b)$ are equal to zero or one for all prime number p. Also, we can assume that $|a| \leq |b|$. We use induction on $m = |a| + |b|$. If $m = 2$, we have

  $$f = X_1^2 \pm X_2^2 \pm X_3^2;$$

  the case of $X_1^2 + X_2^2 + X_3^2$ is excluded because f_{inf} represents zero. Suppose $m > 2$, this means $|b| \geq 2$ and write b in the form

  $$b = \pm p_1 \ldots p_k,$$

  where the p_i are distinct primes. Let p be one of the p_i; we are going to prove that a is a square modulo p. This is obvious if $a \equiv 0 \pmod{p}$. Otherwise a is a p-adic unit, by hypothesis there is $(x, y, z) \in \mathbb{Q}_p^3$ such that $z^2 - ax^2 - by^2 = 0$ and we can suppose that (x, y, z) is primitive. We have $z^2 - ax^2 \equiv 0 \pmod{p}$. From this follows that, if $x \equiv 0 \pmod{p}$, the same is true also for z, and by^2 is divisible by p^2. Since, $\nu_p(b) = 1$ this implies $y \equiv 0 \pmod{p}$ contrary to the fact that (x, y, z) is primitive. Thus we have $x \not\equiv 0 \pmod{p}$, which shows that a is square modulo p. Now,

  $$\mathbb{Z}/b\mathbb{Z} = \prod \mathbb{Z}/p_i\mathbb{Z},$$

  we say that a square modulo b. There exists thus integers t, b' such that

  $$t^2 = a + bb'$$

and we can choose t in such a way that $|t| \leq |b|/2$. The formula $bb' = t^2 - a$ shows that bb' is norm of extension $\mathbb{K}(\sqrt{a})/\mathbb{K}$ where $\mathbb{K} = \mathbb{Q} or \mathbb{Q}_v$; from this we conclude that f represents zero in $\mathbb{K}$ if and only if the same is true for

$$f' = x_1^2 - aX_2^2 - b'X_3^2.$$

In particular, f' represents zero in each of the $\mathbb{Q}_v$, but we have;

$$|b| = \left|\frac{t^2 - a}{b}\right| \leq \frac{|b|}{4} + 1 < |b|,$$

because $|b| \geq 2$. Write b' in the form of b'', u^2 integers and b'' square free; we a $|b''| < |b|$. The induction hypothesis applies thus to the form

$$f'' = X_1^2 - aX_2^2 - b''X_3^2$$

which is equivalent to f', hence this form represents zero in $\mathbb{Q}$ and the same is true for f.

- $n = 4:$
  $f = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2)$. Let $v \in V$. Since f_v represents zero, there exists $x_v \in \mathbb{Q}_v^*$ which represented both by $aX_1^2 + bX_2^2$ and $cX_3^2 + dX_4^2$. This is equivalent to saying that

  $$(x_v, -ab)_v = (a, b)_v \text{ and } (x_v, -cd)_v = (c, d)_v \text{ for all } v \in V.$$

  Since, $\prod(a, b)_v = \prod(c, d)_v = 1$, by Theorem 4.6.1 and obtain from it the existence of $x \in \mathbb{Q}^*$ such that

  $$(x, -ab)_v = (a, b)_v \text{ and } (x, -cd)_v = (c, d)_v \text{ for all } v \in V.$$

  The form $aX_1^2 + bX_2^2 - xZ^2$ represents zero in each of the $\mathbb{Q}_v$, hence in $\mathbb{Q}$. Hence x is represented in $\mathbb{Q}$ by $aX_1^2 + bX_2^2$ and same for $cX_3^2 + dX_4^2$. The fact that f represents zero is follows from this.

- $n = 5:$
  We use induction on n. We write f in the form of $f = h - g$ with $h = a_1X_1^2 + a_2X_2^2, g = -(a_3X_3^2 + \ldots + a_nX_n^2)$ Let S be the subset of V consisting of $\infty, 2$ and the number p such that $\nu_p(a_i) \neq 0$ for one $i \geq 3$; it is finite set. Let $v \in S$. Since f_v represents zero there is $a_v \in \mathbb{Q}_v^*$ which is represented in $\mathbb{Q}_v$ by h and g, there exists $x_i^v \in \mathbb{Q}_v$, $i = 1 \ldots n$ such that

  $$h(x_1^v, x_2^v) = a_v = g(x_3^v, \ldots, x_n^v).$$

  The squares of $\mathbb{Q}_v^*$ forms an open set. Using the approximation theorem this implies existence of x_1, x_2 in $\mathbb{Q}$ such that if $a = h(x_1, x_2)$, one has $a/a_v \in \mathbb{Q}_v^*$ for all $v \in S$. Now, consider the form

$f_1 = aZ^2 - g$. If $v \in S$, g represents a_v in $\mathbb{Q}_v^*$ thus also $a/a_v \in \mathbb{Q}_v^{*2}$; hence f_1 represents zero in $\mathbb{Q}_v$. If $v \notin S$, the coefficients $-a_3, \dots, -a_n$ of g are v-adic units; the same is true for $d_v(g)$ and because $v \neq 2$ we have $\epsilon_v(g) = 1$. In all cases we see that f_1 represents zero in $\mathbb{Q}_v^*$, since the rank of f_1 is $n-1$, the inductive hypothesis shows that f_1 represents zero in $\mathbb{Q}$, that is g represents a in $\mathbb{Q}$, since h represents a, f represents zero, and the proof is complete.

□

Corollary 6.2.2. *Let $a \in \mathbb{Q}^*$. A quadratic form Q over $\mathbb{Q}$ represents a in $\mathbb{Q}$ it is necessary and sufficient that it represents zero in each of the $\mathbb{Q}_v$, where $v \in V$.*

Proof. This follows from the above Theorem6.2.1 to the quadratic form $aZ^2 - Q$. □

Corollary 6.2.3. *A quadratic form of rank greater or equal to 5 represents zero if and only if it is indefinite. i.e. it represents zero in $\mathbb{R}$.*

Proof. Indeed, by Theorem 6.2.1 represents zero in each of the $\mathbb{Q}_p$. □

6.3 Classification

Theorem 6.3.1. *Let f and f' be two quadratic forms over $\mathbb{Q}$. For f and f' to be equivalent over $\mathbb{Q}$, it is necessary and sufficient that they are equivalent over each $\mathbb{Q}_v$.*

Proof. Necessity being trivial, we must show that if f and f' are equivalent over $\mathbb{Q}_v$ for all v, then they are equivalent over $\mathbb{Q}$. The proof is inductive, via Witt's cancellation theorem. The base step, in rank 0, is trivial. So suppose that f, f' have rank $n > 0$, and are equivalent over every $\mathbb{Q}_v$. Choose some $a \in \mathbb{Q}^*$ represented by f. Then a is represented by f' (by a previous corollary to the Hasse-Minkowski Theorem). Thus we may write $f \sim aZ^2 + g$ and $f' \sim aZ^2 + g'$, for some quadratic forms g, g' over $\mathbb{Q}$. By Witt's cancellation theorem, this implies that $g \sim g'$ over every $\mathbb{Q}_v$, since $f \sim f'$ over every $\mathbb{Q}_v$. By induction, $g \sim g'$ over $\mathbb{Q}$. Hence $f \sim f'$ over $\mathbb{Q}$ as well.

□

Corollary 6.3.2. *Let (r, s) and (r', s') be the signatures of f and f'. For f and f' to be equivalent it is necessary and sufficient that one has;*

$$\textit{rank}(f) = \textit{rank}(f'), d(f) = d(f'), (r, s) = (r', s') \textit{ and } \epsilon_v(f) = \epsilon_v(f').$$

Proof. f and f' are equivalent over each $\mathbb{Q}_v$. Also, these invariants are not arbitrary but we can say they have restriction over them and all verifies following relations.

1) $\epsilon_v = 1$ for almost all $v \in V$ and $\prod_{v \in V} \epsilon_v = 1$,

2) $\epsilon_v = 1$ if $n = 1$ or if $n = 2$ and if image d_v of d in $\mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$ is equal to -1,

3) $r, s \geq 0$ and $r + s = n$,

4) $d_\infty = (-1)^s$,

5) $\epsilon_\infty = (-1)^{s(s-1)/2}$.

□

Proposition 6.3.3. *Let $d, (\epsilon_v)_{v \in V}$ and (r, s) satisfy the relations above. Then exists a quadratic form of rank of n over $\mathbb{Q}$ having for invariants $d, (\epsilon_v)_{v \in V}$ and (r, s).*

Proof. For $n = 1$, proposition is trivial.
Suppose that $n = 2$. Let $v \in V$. The non-degeneracy of Hilbert symbol with 2^{nd} condition, shows that there is $x_v \in \mathbb{Q}_v^*$ such that $(x_v, -d)_n = \epsilon_v$. Also, form first condition existence of $x \in \mathbb{Q}^*$ such that $(x, -d)_v = \epsilon_v$ for all $v \in V$, then $xY^2 + xdZ^2$ works.
Suppose $n = 3$. Let $S = \{v \in V : (-d, -1)_v = -\epsilon_v\}$. It is easy to see that the set S is finite. If $v \in V$, choose in $\mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$ an element c_v from distinct from the image $-d_v$ of $-d$ in this group. By using approximation theorem 3.2.5, it is easy to see that there exists $c \in \mathbb{Q}^*$ whose image in each of the $\mathbb{Q}_v^*/\mathbb{Q}_v^{*2}, v \in S$, is c_v. Just now we proved proved existence of a from form of rank 2 such that

$$d(g) = cd, \ \epsilon_v(g) = (c, -d)_v \epsilon_v, \ \text{for all } v \in V.$$

Then quadratic form $f = cZ^2 + g$ works.
When $n \geq 4$ we use induction on n. Suppose first that $r \geq 1$. By using inductive hypothesis, we obtain a form g of rank $n - 1$ which has invariants $d, (\epsilon_v)_{v \in V}$ and $(r - 1, s)$. Then quadratic form $X^2 + g$ will works. When $r = 0$, we use a form h of rank $n - 1$ having for invariants $-d, \epsilon_v(-1, -d)_v$ and $(0, n - 1)$ the form $-X^2 + h$ works. □

Bibliography

[Ser73] Serre, J.-P. A course in arithmetic. Springer-Verlag, 1973.

[DF] DF Dummit, D. and Foote, R. Abstract algebra. John Wiley & Sons Inc., 2004.

[Hun73] Hungerford, T. Algebra. Springer-Verlag, 2003.