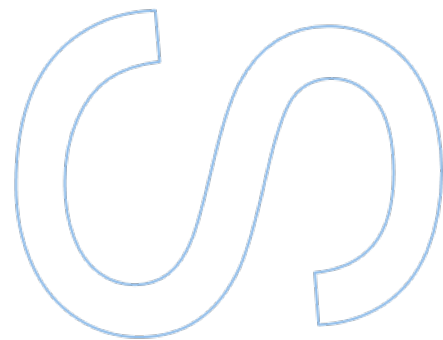
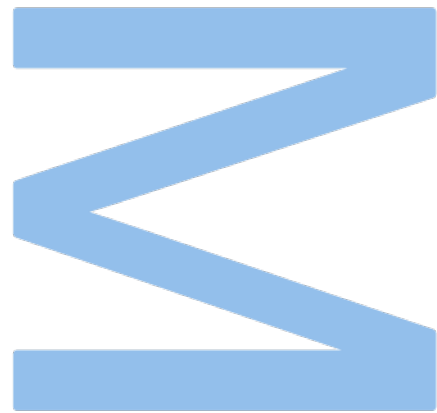
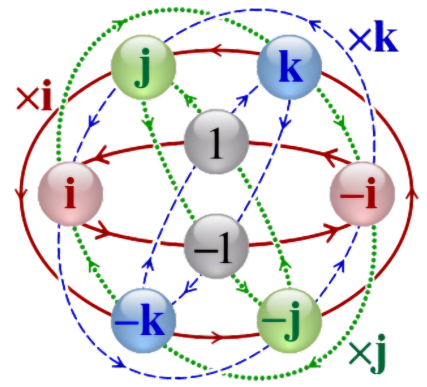


The Metacommutation Problem in the Hurwitz Integers



António Leite

Mestrado em Matemática
Departamento de Matemática
Faculdade de Ciências da Universidade do Porto
2024



The Metacommutation Problem in the Hurwitz Integers

António Leite

Dissertação realizada no âmbito do Mestrado em
Matemática
Departamento de Matemática
2024

Orientador

António Machiavelo, Professor Auxiliar,
Faculdade de Ciências da Universidade do Porto

Acknowledgments

Last year I had the incredible privilege of working in the field of Mathematics I always dreamed. This opportunity was largely due to professor António Machiavelo, to whom I extend my thanks for allowing me to work under his guidance. His crucial advice, patience, and insightful conversations were invaluable in the writing of this text. I would also like to thank all the professors I encountered during my academic journey at FCUP.

I am profoundly grateful to my family for their unwavering encouragement and support throughout the years. In particular, I would like to thank my father for being the first person to show me the beauty of Mathematics, and my mother for raising me in a way that no one else could.

A special thanks goes to all my friends who, over the past year, checked in on me and took the time to share a cup of coffee. In particular, I would like to thank João for always keeping me alive outside of this, and providing the support I needed.

I am deeply thankful to Rodrigo and Rui, for being the best companions on this journey that is studying Mathematics.

Finally, I wish to express my gratitude to the most amazing person I know, Luísa. Thank you for always being there for me and showing me how beautiful life can be by your side.

“There are a million Paths in this world, Lindon, but any sage will tell you they can all be reduced to one. Improve yourself.” - <i>Suriel in Unsouled</i> by Will Wight

Resumo

Os anéis dos inteiros de Lipschitz e dos inteiros de Hurwitz são dois anéis da álgebra dos quatérnios que são intrigantes do ponto de vista aritmético. Nos Inteiros de Hurwitz, existe uma espécie de propriedade única de fatorização que motiva um problema denominado problema da metacomutação, apontado por Conway e Smith. Nesta tese estudamos algumas propriedades da metacomutação, seguindo os resultados recentes de H. Cohn e A. Kumar. Começamos por fazer uma revisão dos preliminares necessários, em particular, de resultados clássicos de Lipschitz, Hurwitz e G. Pall. Em seguida, apresentamos o problema da metacomutação e definimos o mapa de metacomutação, que é uma permutação. Isto permite-nos tirar conclusões sobre o número de pontos fixos e o sinal da permutação. Posteriormente, provamos o principal resultado desta tese, de que existe um critério para saber se os ciclos que não são pontos fixos possuem um determinado comprimento. No final, estudamos algumas propriedades dos divisores comuns à esquerda e à direita de um inteiro de Hurwitz.

Palavras-chave: Quatérnios, Inteiros de Lipschitz, Inteiros de Hurwitz, Fatorização, Problema da Metacomutação.

Abstract

The rings of Lipschitz Integers and Hurwitz Integers are two rings of the quaternion algebra which are intriguing from the arithmetical points of view. In the Hurwitz Integers, there exists a sort of unique factorization property that motives a problem called the metacommutation problem, which was pointed out by Conway and Smith. In these thesis, we study some properties of the metacommutation, following the recent results of H. Cohn and A. Kumar. We start by doing a revision of the necessary preliminaries, in particular, the classic results from Lipschitz, Hurwitz and G. Pall. Then, we introduce the metacommutation problem, and define the metacommutation map, which is a permutation. This allows us to derive conclusions about the number of fixed points and the sign of the permutation. Afterwards, we prove the main result of this thesis, that there is a criteria to know whether the cycles which are not fixed points have a given length. At the end, we study some properties of the common left and right-hand divisors of a Hurwitz integer.

Keywords: Quaternions, Lipschitz Integers, Hurwitz Integers, Factorization, Metacommutation Problem.

Table of Contents

Acknowledgments	III
Resumo	V
Abstract	VII
Introduction	1
1 Preliminaries	5
1.1 The quaternions	5
1.1.1 Lipschitz and Hurwitz integers	7
1.1.2 Number of primes that lie above p	11
1.2 Finite fields	16
1.2.1 Generalities and field extensions	17
1.2.2 Structure of finite fields	20
1.2.3 Cyclotomic polynomials	23
1.3 Quadratic forms	24
1.3.1 Quadratic forms over finite fields	30
1.4 The projective space	31
1.4.1 Projective curves: Conics	34
2 The Metacommutation Problem	39
2.1 Metacommutation map	39
2.2 A conic associated to the primes above p	41
2.3 Metacommutation revisited	43
2.4 Fixed points	45
2.5 Cycle structure and sign of permutation	48
3 On the cycle structure of the Metacommutation map	55
3.1 Cycles of length 4 and 6	55
3.2 A generalization	60
3.3 Common left and right-hand divisors of a quaternion integer	62
3.3.1 Fixed points revisited	64

A Semisimplicity	69
B SageMath auxiliar code	71
Bibliography	73

Introduction

In modern days, the **Hamilton Quaternions**,

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\},$$

are not as exotic as they used to be. There are various applications of quaternions to different branches of science such as mechanics, geometry, number theory, and even computational animations. Even though the connections between quaternions and number theory are not usually glanced as the pinnacle of its applications, the quaternions are of great interest from the arithmetical point of view. Particularly intriguing is the ring of **Lipschitz integers**,

$$\mathcal{L} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z}\},$$

and the ring of **Hurwitz integers**,

$$\mathcal{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z} \text{ or } a, b, c, d \in \frac{1}{2} + \mathbb{Z}\}.$$

The first ones, as the name suggests, were studied by Rudolf Lipschitz, namely in [Lip86], in which he proved different properties about this ring. Given a quaternion $\alpha = a + bi + cj + dk \in \mathbb{H}$, its **conjugate** is $\bar{\alpha} = a - bi - cj - dk$, and its **norm** is $N(\alpha) = a^2 + b^2 + c^2 + d^2$. One of the properties that Lipschitz proved is the fact that the number of Lipschitz integers with norm equal to a rational prime p is $p + 1$, up to left multiplication by units (elements with norm equal to 1). However, it is not possible to perform Euclidean division in the ring of Lipschitz integers. Hence, to solve this issue, Adolf Hurwitz studied the Hurwitz integers. In fact, this ring is left (or right) Euclidean, and so every left (or right) ideal is principal, and as a consequence of the existence of the Euclidean algorithms, it can be shown that any non-zero $h \in \mathcal{H}$ with norm $N(h) = p_1 p_2 \cdots p_n$, where p_i are prime, can be factored as:

$$h = P_1 P_2 \cdots P_n, \quad \text{where } N(P_i) = p_i.$$

As Conway and Smith denoted in [CS03], we say that this factorization of x is modeled on a factorization of $N(h) = p_1 \cdots p_n$. When h is not a multiple of an integer greater than 1, this factorization is unique up to unit migration, that is, every factorization of x modeled on $N(h)$ (where order matters) is of the form:

$$h = (P_1 u_1)(u_1^{-1} P_2 u_2) \cdots (u_{n-1}^{-1} P_n), \quad \text{where } N(P_i) = p_i.$$

If we consider the case $N(h) = pq$, where p and q are distinct rational primes, then $h = PQ$ has a unique factorization $Q'P'$ modeled on qp , up to unit migration. This process of swapping

primes was called **metacommutation** by Conway and Smith, in [CS03]. In fact, they proved that the prime factorization of an arbitrary Hurwitz integer is unique up to metacommutation, unit migration and recombination: which is when, in a factorization, we replace $P\bar{P}$ with $P_1\bar{P}_1$, where $N(P) = N(P_1)$. Even though we have a factorization in Hurwitz integers that is unique up to metacommutation, this does not mean that it is unique in the usual sense. That would imply solving the **metacommutation problem**, that is, how does a factorization PQ modeled on pq determines the corresponding factorization $Q'P'$ modeled on pq . Thus, if we fix a $Q \in \mathcal{H}$ with norm q and p a rational prime, every prime P with norm p has an associated P' which satisfies $PQ = Q'P'$ for some $Q' \in \mathcal{H}$.

Therefore, metacommutation by Q induces a permutation $\tau_{Q,p}$, which we call the **metacommutation map** of the Hurwitz primes of norm p . Recently, in [CK15], Cohn and Kumar proved that the sign of the permutation is $\left(\frac{q}{p}\right)$, and if the permutation is not the identity, then the number of fixed points of $\tau_{Q,p}$ is $1 + \left(\frac{a^2 - q}{p}\right)$. This is the main motivation of this text, where we address some of the work by Lipschitz and Hurwitz, and also prove and explain in detail the recent results present in [CK15].

Structure of the text

In Section 1 we introduce the necessary preliminaries needed to understand the rest of the text. We start with a revision of elementary concepts about quaternions, and then prove some properties about Lipschitz and Hurwitz integers, namely that there is a sort of unique factorization in the Hurwitz integers and that the number of primes that lie above p is, up to left multiplication by units, $p+1$. We also present a result from Gordon Pall about the right divisors of a quaternion. We then move to a review of finite fields, recalling generalities about finite field extensions, which allows us to define and prove properties about cyclotomic polynomials over finite fields. These constructions will be needed in the proof of Theorem 3.7 of Chapter 3. Afterwards, we recall the notion of projective space where, in particular, we prove that there is a bijection between nondegenerate conics over the projective plane and the projective line, this is fundamental to understand the metacommutation map in Chapter 2. We end this section by reviewing the basics of quadratic forms, mainly quadratic forms over finite fields, which is needed in order to determine the sign of the metacommutation map.

Section 2 is devoted to the study of the metacommutation problem. We first introduce this problem, and then move to the metacommutation map. We are interested in proving results about its cycle structure, in particular the number of fixed points, the sign of permutation and the length of cycles which are not fixed points.

In Section 3 lies the main result of this text, where we build upon the results of Chapter 2, and prove that there is a criteria to know whether the cycles which are not fixed points have a given length. We start this section by analyzing a criteria to decide if the non-trivial cycles have length 4 or length 6, which will allow us to generalize this to all lengths. Then, we are interested in studying left and right-hand factors of a quaternion integer, namely when this quaternion is a product of two primes P and Q , since they will give us a different way of look at the fixed

points of our metacommutation map.

To conclude, we present in Appendices A and B, respectively, some concepts about semisimplicity that are used in Chapter 2, and auxiliary functions used in Chapter 3.

Chapter 1

Preliminaries

In this chapter, we provide the reader with the basic notions needed to understand the concepts that appear in later chapters. We start by giving some introductory definitions about quaternions, proving some elementary properties, and then move to the subrings of Lipschitz and Hurwitz integers. We prove that there is a sort of unique factorization property in Hurwitz integers, and study the number of primes that lie above a rational prime p . Then, we present some important notions about finite fields, quadratic forms, and the projective space which will be helpful in Chapter 2.

1.1 The quaternions

The ring of **Hamilton quaternions**, denoted by $\mathbb{H}$, is defined as:

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}.$$

This ring is, in fact, a division algebra with pointwise addition and its product is determined by this relation on the basis elements i, j and k :

$$i^2 = j^2 = k^2 = ijk = -1.$$

An important thing to notice is that this product is **not commutative**, as, for example, $ij = k$, but $ji = -k$.

Let $u = u_0 + u_1i + u_2j + u_3k$ and $v = v_0 + v_1i + v_2j + v_3k$. The product of u by v , in that order, can be explicitly written as:

$$\begin{aligned} uv &= (u_0 + u_1i + u_2j + u_3k)(v_0 + v_1i + v_2j + v_3k) = \\ &= (u_0v_0 - u_1v_1 - u_2v_2 - u_3v_3) + (u_0v_1 + u_1v_0 + u_2v_3 - u_3v_2)i + \\ &\quad (u_0v_2 - u_1v_3 + u_2v_0 + u_3v_1)j + (u_0v_3 + u_1v_2 - u_2v_1 + u_3v_0)k. \end{aligned} \tag{1.1}$$

Definition 1.1. Let $u = a + bi + cj + dk \in \mathbb{H}$. Then:

1. $\bar{u} = a - bi - cj - dk$, is the conjugate of u ,
2. $\Re(u) := \frac{1}{2}(u + \bar{u}) = a$, is the real part of u ,
3. $\mathcal{V}(u) := \frac{1}{2}(u - \bar{u}) = bi + cj + dk$, is the vector part of u ,
4. if $\Re(u) = 0$, we say that u is pure.

We can identify the set of pure quaternions, as a vector space, with $\mathbb{R}^3$. Then, from the explicit expression in 1.1, we notice that $\mathcal{V}(u)\mathcal{V}(v) = -\mathcal{V}(u) \cdot \mathcal{V}(v) + \mathcal{V}(u) \times \mathcal{V}(v)$, where $\cdot$ denotes the usual inner product and $\times$ the usual cross product. This gives us new a way of looking at the product of two quaternions.

Proposition 1.2. Let $u, v \in \mathbb{H}$. Then $uv = \Re(u)v + \Re(v)u - u \cdot v + \mathcal{V}(u) \times \mathcal{V}(v)$.

Proof.

$$\begin{aligned}
 uv &= (\Re(u) + \mathcal{V}(u))v \\
 &= \Re(u)v + \mathcal{V}(u)\Re(v) + \mathcal{V}(u)\mathcal{V}(v) \\
 &= \Re(u)v + \Re(v)\mathcal{V}(u) - \mathcal{V}(u) \cdot \mathcal{V}(v) + \mathcal{V}(u) \times \mathcal{V}(v) \\
 &= \Re(u)v + \Re(v)\mathcal{V}(u) + \Re(v)\Re(u) - \Re(v)\Re(u) - \mathcal{V}(u) \cdot \mathcal{V}(v) + \mathcal{V}(u) \times \mathcal{V}(v) \\
 &= \Re(u)v + \Re(v)u - u \cdot v + \mathcal{V}(u) \times \mathcal{V}(v).
 \end{aligned}$$

□

From this, we get a relation between $\overline{uv}$, $\bar{u}$ and $\bar{v}$.

Proposition 1.3. Let $u, v \in \mathbb{H}$. Then $\overline{uv} = \bar{v}\bar{u}$.

Proof.

$$\begin{aligned}
 \overline{uv} &= \Re(u)\bar{v} + \Re(v)\bar{u} - u \cdot v - \mathcal{V}(u) \times \mathcal{V}(v) \\
 &= \Re(\bar{u})\bar{v} + \Re(\bar{v})\bar{u} - \bar{u} \cdot \bar{v} + \mathcal{V}(\bar{v}) \times \mathcal{V}(\bar{u}) \\
 &= \bar{v}\bar{u}.
 \end{aligned}$$

□

Again, we can see from 1.1, that $\Re(uv) = u \cdot \bar{v}$. Thus, we have that $u \cdot v = \Re(u\bar{v}) = \frac{1}{2}(u\bar{v} + v\bar{u})$, and it also follows, for all $u, v, \alpha \in \mathbb{H}$,

$$u\alpha \cdot v = \Re((u\alpha)\bar{v}) = \Re(u(\alpha\bar{v})) = u \cdot \overline{\alpha\bar{v}} = u \cdot v\bar{\alpha}.$$

Similarly, $\alpha u \cdot v = u \cdot \bar{\alpha}v$. With this in mind, we can write all the coordinates of uv using only the inner product.

Proposition 1.4. *Let $u, v \in \mathbb{H}$. Then $uv = (u \cdot \bar{v}) + (u \cdot i\bar{v})i + (u \cdot j\bar{v})j + (u \cdot k\bar{v})k$.*

Proof. It is easy to notice that we have $uv \cdot i = u \cdot i\bar{v}$. The other cases are similar. $\square$

Remark 1.5. Notice that, using Proposition 1.2, it is a straightforward computation to see that $uv - vu = 2\mathcal{V}(u) \times \mathcal{V}(v)$, which shows that two quaternions commute if and only if their vector parts are colinear.

Definition 1.6. Let $u = a + bi + cj + dk \in \mathbb{H}$. Define:

1. $N(u) = u\bar{u} = a^2 + b^2 + c^2 + d^2$, the norm of u ,
2. $\text{Tr}(u) = u + \bar{u} = 2\Re(u)$, the trace of u .

Remark 1.7. Since $u \cdot v = \frac{1}{2}(u\bar{v} + v\bar{u})$, we have that $u \cdot u = u\bar{u} = N(u)$.

Proposition 1.8. *The norm is a multiplicative function and the trace is $\mathbb{R}$ -linear.*

Proof. Given $u, v \in \mathbb{H}$,

$$N(uv) = uv\bar{u}\bar{v} = uv\bar{v}\bar{u} = uN(v)\bar{u} = N(u)N(v),$$

and for any $x, y \in \mathbb{R}$,

$$\text{Tr}(xu + yv) = (xu + yv) + \overline{xu + yv} = x(u + \bar{u}) + y(v + \bar{v}) = x\text{Tr}(u) + y\text{Tr}(v)$$

$\square$

1.1.1 Lipschitz and Hurwitz integers

In this thesis, there are two subrings of $\mathbb{H}$ - the Lipschitz integers and the Hurwitz integers - which are of most interest to us, since they have useful arithmetical properties from the Number Theory point of view. For example, we can use their arithmetic to prove that every natural number can be written as a sum of four natural squares numbers (see, for example, [CP12]). We will work mainly in these subrings, therefore it is fundamental to present some background.

Definition 1.9. The ring of **Lipschitz integers**, denoted by $\mathcal{L}$, is defined as,

$$\mathcal{L} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z}\}.$$

It is important to notice that, in Number Theory, this subring is interesting because the norm of every one of its elements is always a natural number. However, if we look at the ideal generated by $\langle 1 + i, 1 - j \rangle$, it is not difficult to see that this ideal is not principal, as it is easy to see that any of its elements has norm 2. Therefore, the ring of Lipschitz integers is not a left (or right) principal ideal domain, and as a consequence it cannot be left (or right) Euclidean. Thus, we need to use some ring that still has a natural norm for its elements, but has better properties to work with.

Definition 1.10. The ring of **Hurwitz integers**, denoted by $\mathcal{H}$, is defined as

$$\mathcal{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z} \text{ or } a, b, c, d \in \frac{1}{2} + \mathbb{Z}\}.$$

Let us see that, in fact, the norm of a Hurwitz integer is always a natural number. The case where $u \in \mathcal{L}$ is trivial, so let $u \in \mathcal{H} \setminus \mathcal{L}$, then $u = \frac{a}{2} + \frac{b}{2}i + \frac{c}{2}j + \frac{d}{2}k$ and $a, b, c, d \in \mathbb{Z}$, with $a \equiv b \equiv c \equiv d \equiv 1 \pmod{2}$. This implies that $a^2 \equiv b^2 \equiv c^2 \equiv d^2 \equiv 1 \pmod{4}$, so $N(u) \equiv 0 \pmod{4}$, meaning that the norm of every Hurwitz integer is always a natural number.

Definition 1.11. Given $u \in \mathcal{H}$, we say that u is a unit if there exists $u' \in \mathcal{H}$ such that $uu' = 1$. We denote the set of all units as $\mathcal{H}^*$.

Remark 1.12. It is easy to see that $u \in \mathcal{H}^* \Leftrightarrow \exists u' : uu' = 1 \Leftrightarrow N(u) = 1$. This follows from the fact that the norm of u is always a natural number, and $N(u) = 1 \Leftrightarrow u\bar{u} = 1$. Therefore, the units in $\mathcal{H}$ are precisely the elements of norm 1.

Let us now find the units of the Lipschitz and Hurwitz integers.

Proposition 1.13. The ring $\mathcal{H}$ has 24 units: the 8 from $\mathcal{L}$, $\{\pm 1, \pm i, \pm j, \pm k\}$, and the 16 elements of $\left\{\frac{\pm 1 \pm i \pm j \pm k}{2}\right\}$.

Proof. The Lipschitz units are easy to see.

Let $u = a + bi + cj + dk \in \mathcal{H} \setminus \mathcal{L}$ be a unit. We know that $N(u) = 1 \Leftrightarrow a^2 + b^2 + c^2 + d^2 = 1$ and since $a, b, c, d \in \frac{1}{2} + \mathbb{Z}$, if $|a| > \frac{1}{2}$, then $|a| \geq \frac{3}{2}$, so $a^2 \geq \frac{9}{4}$, and $N(u) > 1$, which is not possible. So $|a| = \frac{1}{2}$. But, by the same argument, $|b| = |c| = |d| = \frac{1}{2}$. □

Definition 1.14. Given $u, v \in \mathcal{H}$, we say that v is a left (right) divisor of u , and put $v \rfloor u$ ($v \lceil u$), if there exists $w \in \mathcal{H}$ such that $u = vw$ ($u = wv$).

We say that two quaternions $u, v \in \mathcal{H}$ are **left associates** if $u \rfloor v$ and $v \lceil u$, i.e., we can obtain u by multiplying v by an unit. The definition of **right associate** is analogous.

Definition 1.15. A Hurwitz integer is called **irreducible** if it is neither 0 nor a unit, and it is not a product of non-units.

Remark 1.16. As a convention we call the irreducible quaternions, **prime quaternions**, even though they are not prime in the usual sense, since it is possible to find an irreducible quaternion q such that $q \rfloor ab$, but we do not have either $q \rfloor a$ or $q \rfloor b$. For example, if $P = 1 + j$ and $Q = 2 + i$, then $PQ = 2 + i + 2j - k = (2 - k)P$ and P and Q are prime quaternions, however $(2 - k)$ does not divide Q nor P .

The next proposition about Hurwitz integers does not apply to the Lipschitz ones.

Proposition 1.17. The ring $\mathcal{H}$ is left (or right) Euclidean.

Proof. Given $u, v \in \mathcal{H}$, define $w = v^{-1}u = (\bar{v}u)/N(v) \in \mathbb{H}$. Then let $q \in \mathcal{L}$ be the quaternion built from w by taking the integers closer to its coordinates.

Put $s = w - q$, then $N(s) \leq 4 \left(\frac{1}{2}\right)^2 = 1$. If we put $r = vs = u - vq \in \mathcal{H}$, then $u = vq + r$, and we have $N(r) = N(v)N(s) \leq N(v)$. If $N(s) < 1$ then $N(r) < N(v)$ and if $N(s) = 1$, then $s = \frac{\pm 1 \pm i \pm j \pm k}{2} \in \mathcal{H}$, and so $s = w - q \in \mathcal{H}$, thus $w = v^{-1}u = q + s \in \mathcal{H}$, therefore v divides u from the left. $\square$

It is a well known result that every left (or right) Euclidean Domain is and left (or right) Principal Ideal domain. Therefore, one has:

Corollary 1.18. *The ring $\mathcal{H}$ is a left (or right) Principal Ideal Domain.*

Since $\mathcal{H}$ is non commutative, we do not have a unique factorization in the normal sense (like in the integers). Nonetheless we have a weaker result, that still holds a crucial place in the next chapters.

Definition 1.19. An element $h \in \mathcal{H}$ is called **primitive** if it cannot be divided by a rational prime, i.e., it cannot be written as $h = mq$, where $m \in \mathbb{Z} \setminus \{\pm 1\}$ and $q \in \mathcal{H}$.

Theorem 1.20 (Unique Factorization theorem). *Let Q be a primitive Hurwitz integer with norm $N(Q) = q$. To each factorization of the norm q into a product of $p_0 p_1 \cdots p_k$ rational primes, where order matters, there is a factorization of Q ,*

$$Q = P_0 P_1 \cdots P_k,$$

modeled on that factorization on q , that is, with $N(P_i) = p_i$.

Moreover, if $Q = P_0 P_1 \cdots P_k$ is any factorization modelled on $p_0 p_1 \cdots p_k$, then any other factorization is of the form

$$Q = P_0 U_1 \cdot U_1^{-1} P_1 U_2 \cdot U_2^{-1} P_2 \cdots U_k \cdot U_k^{-1} P_k,$$

which means that the factorization on a given model is “unique to unit-migration”.

The proof of this theorem is essentially the one present [CS03] with some slight alterations.

Proof. Let $Q \in \mathcal{H}$ be primitive with $N(Q) = q = p_0 p_1 \cdots p_k$, and consider the right ideal $p_0 \mathcal{H} + Q \mathcal{H}$. Since $\mathcal{H}$ is a left principal ideal domain, this ideal must be equal to $P_0 \mathcal{H}$, for some $P_0 \in \mathcal{H}$, unique up to right multiplication by units. Then, for some $h \in \mathcal{H}$, we must have that $p_0 = P_0 h$ and so $N(p_0) = p_0^2 = N(P_0) N(h)$, which means that the norm of P_0 must divide p_0^2 . From this, we see that $N(P_0)$ must be 1, p_0 or p_0^2 . If $N(P_0) = 1$, then $p_0 \mathcal{H} + Q \mathcal{H} = \mathcal{H}$, but that cannot be since an arbitrary element $h = p_0 a + Q b$ has norm

$$\begin{aligned} N(h) &= (p_0 a + Q b) \overline{(p_0 a + Q b)} = N(p_0) N(a) + p_0 [a \overline{Q b} + Q b \overline{a}] + N(Q) N(b) \\ &= p_0^2 N(a) + p_0 [a \overline{Q b} + Q b \overline{a}] + p_0 p_1 \cdots p_k N(b), \text{ which is divisible by } p_0. \end{aligned}$$

If $N(P_0) = p_0^2$, from $p_0^2 = N(P_0) N(h)$, we would have that $N(h) = 1$, so h be an unit, therefore $P_0 = p_0 h^{-1}$, which means that p_0 must divide Q , which is a contradiction since we are assuming that Q is primitive.

Therefore, we must have that $N(P_0) = p_0$. Thus, P_0 is a Hurwitz prime, which is unique up to right multiplication by units, and divides Q . So exists $Q_1 \in \mathcal{H}$ such that $Q = P_0 Q_1$, with $N(Q_1) = p_1 p_2 \cdots p_k$. Now, taking Q_1 , we can repeat the process for the ideal $p_1 \mathcal{H} + Q_1 \mathcal{H} = P_1 \mathcal{H}$ and show that $Q_1 = P_1 Q_2$, with $N(Q_2) = p_2 \cdots p_k$. If we repeat the process for the remaining indexes, we obtain, by the same argument, that $Q = P_0 P_1 \cdots P_k$, where $N(P_i) = p_i$, where all the p_i are primes.

□

This theorem is weaker than the one we have for the integers, $\mathbb{Z}$, since the unique factorization property of an Hurwitz integer only holds true for a fixed order of the factorization of its norm. As an example consider $\alpha = 1 + 4i + 3j - 2k$. Then the factorization of α modeled on $N(\alpha) = 2 \times 3 \times 5$ is, up to unit migration, $\alpha = (1 + j)(1 + i + j)(2 + k)$, while the factorization modeled on $N(\alpha) = 5 \times 2 \times 3$ is $\alpha = (-2 - j)(i - k)(-1 + i - j)$.

Conway and Smith also proved the following lemma in [CS03].

Lemma 1.21. *Any factorization of a Lipschitz integer into Hurwitz integers is equivalent by unit-migration to one into Lipschitz integers.*

Proof. See Lemma 1 of [CS03, page 63].

□

Proposition 1.22. *An element $h \in \mathcal{H}$ is prime if and only if its norm is a rational prime.*

Proof. If h is not a prime then it must be a product of two non-units, and so its norm cannot be a rational prime. If its norm is not a rational prime, then its prime factorization has at least two primes, that would correspond to two Hurwitz primes in the factorization of h , so h cannot be prime.

□

Another fundamental result, first proved by Gordon Pall (see [Pal40]) for odd Lipschitz integers, is the following, of which we provide a completely arithmetical proof, due to A. Machiavello.

Theorem 1.23. *Let $u \in \mathcal{L}$ be a primitive quaternion, and let $m \in \mathbb{N}$ be such that $m \mid N(u)$.*

Then there is only one right divisor of u of norm m , up to left associates.

Proof. Let $v \in \mathcal{L}$ be such that $\mathcal{H}u + \mathcal{H}m = \mathcal{H}v$, and let $\alpha, \beta \in \mathcal{H}$ be such that $v = \alpha u + \beta m$. Then $N(v) = (\alpha u + \beta m)(\bar{u}\bar{\alpha} + \bar{\beta}\bar{m}) = N(\alpha)N(u) + m^2 N(\beta) + (\alpha u \bar{\beta} + \beta \bar{u} \bar{\alpha})m$ is divisible by m , by hypothesis. Let $t \in \mathbb{N}$ be such that $N(v) = mt$.

Since $u, m \in \mathcal{H}v$, there are $f, g \in \mathcal{H}$ such that $u = fv$ and $m = gv$. Then $m^2 = N(g)N(v) = N(g)mt$, and thus $m = N(g)t$, from which it follow that $gv = m = N(g)t = g\bar{g}t$, and so $v = \bar{g}t$. But then $u = fv = f\bar{g}t$ implies that $t \mid u$, from which it follows that $t = 1$, since u is primitive. This shows that $N(v) = m$, proving that u does have a right divisor norm m .

Now, if w is another right divisor of u of norm m , then $u = \sigma w$, for some $\sigma \in \mathcal{H}$. But then $v = \alpha \sigma w + \beta \bar{w}w = (\alpha \sigma + \beta \bar{w})w$. The fact that $N(v) = N(w)$ then entails that w and v are left associates.

□

Imagine that we have a quaternion h such that $N(h) = p_1 p_2 p_3$, with p_1, p_2, p_3 different rational primes. Then, from Theorem 1.20, there exists a factorization of $h = P_1 P_2 P_3$, with $N(P_i) = p_i$. However, if we use $N(h) = p_2 p_1 p_3$, we also have that $h = P'_2 P'_1 P'_3$. Theorem 1.20 does not relate P_3 with P'_3 , but with Theorem 1.23 in mind, we have that P_3 and P'_3 are left associates.

Proposition 1.24. *Every element of $\mathcal{H}$ has a right and left associate in $\mathcal{L}$.*

Proof. Let $h = \frac{a + bi + cj + dk}{2} \in \mathcal{H} \setminus \mathcal{L}$. Since the a, b, c, d are all odd, we must have

$$a = 4a' + u_1, \quad b = 4b' + u_2 \quad c = 4c' + u_3 \quad d = 4d' + u_4,$$

where $a', b', c', d' \in \mathbb{Z}$ and $u_i = \pm 1$, for $i = \{1, 2, 3, 4\}$. Therefore,

$$h = 2(a' + b'i + c'j + d'k) + \frac{u_1 + u_2i + u_3j + u_4k}{2},$$

notice that $u = \frac{u_1 + u_2i + u_3j + u_4k}{2} \in \mathcal{H}^* \setminus \mathcal{L}^*$. Then, $\bar{u}h \in \mathcal{L}$. □

Lemma 1.25. *Let p be an odd prime and $Q, P, B \in \mathcal{H}$. Assume that $p \mid QPB$, where $N(P) = p$. If $p \nmid QP$, then $p \mid PB$.*

This is the essentially the same as the second proof of Lemma 4.2 presented in [CP12].

Proof. Consider the ideal $\bar{P}\mathcal{H} + B\mathcal{H}$. Since $\mathcal{H}$ is a left principal ideal, one has $\bar{P}\mathcal{H} + B\mathcal{H} = \alpha\mathcal{H}$, for some $\alpha \in \mathcal{H}$. Notice first that $N(\alpha) \mid N(\bar{P}) = p$, since $\bar{P} = \alpha h$, for some $h \in \mathcal{H}$. Therefore, $N(\alpha)$ is 1 or p . However, α cannot be a unit, since that would imply that there exists $x, y \in \mathcal{H}$ such that,

$$\bar{P}x + By = 1 \Rightarrow QP(\bar{P}x + By) = QP,$$

so p would divide QP , but that cannot be by hypothesis. Hence, $\alpha = \bar{P}u$, for some unit u , and so $B = \bar{P}\beta$, for some $\beta \in \mathcal{H}$. Thus, we have $p \mid P\bar{P}\beta = PB$. □

1.1.2 Number of primes that lie above p

In the final part of this section we prove an important result about the Lipschitz quaternions, namely that for a p prime, there are $p + 1$ Lipschitz primes up to associates that lie above p . The contents of this section are adapted from Lipschitz's original work, in particular section IV, V and VI of [Lip86], and a more recent approach present in [Per11].

We say a prime P **lies above** the rational number p if $N(P) = p$, and we say a Lipschitz quaternion $u = a + bi + cj + dk$ is **proper** if $(a, b, c, d) = 1$.

When a congruence is verified by a solution of integers (x, y, z) that are not all divisible by p , we say that solution is a **proper solution** of the congruence. Our first problem is determining the number of proper solutions of the congruence:

$$x^2 + y^2 + z^2 \equiv 0 \pmod{p}. \tag{1.2}$$

Two solutions (x, y, z) and (x', y', z') are **equivalent** if there exists a nonzero $a \in \mathbb{F}_p$ such that $x' = ax$, $y' = ay$ and $z' = az$. We denote $[x, y, z]$ this class of solutions, as the relation we just introduced is an equivalence relation. We start by considering the solutions where z is not divisible by p . These solutions can be reduced to the case where $z = 1$, since given any such solution (x, y, z) , where z is not divisible by p , we have an equivalent solution $(x', y', 1)$ dividing all coordinates by z . For $z = 1$ the congruence 1.2 is equivalent to:

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}. \quad (1.3)$$

The study of this congruence, as we will see in the next theorem, can be reduced to the study of the congruence:

$$1 + a^2 \equiv b^2 \pmod{p}. \quad (1.4)$$

Therefore, we start by studying it instead.

Lemma 1.26. *The congruence $1 + a^2 \equiv b^2 \pmod{p}$ has precisely $p - 1$ solutions over $\mathbb{F}_p$.*

Proof. We can write the given congruence as

$$1 \equiv (b - a)(b + a) \pmod{p}.$$

If we let

$$b - a = r, \quad b + a = s, \quad (1.5)$$

then the congruence is simply,

$$1 \equiv rs \pmod{p}. \quad (1.6)$$

This congruence shows that r is a unit and $r^{-1} = s$, in $\mathbb{F}_p$. Since there are $p - 1$ units, if we take r as each one of them, we can determine the corresponding value of s . Thus, we have that the congruence 1.6 has $p - 1$ solutions, and there exist a bijection between this solutions and the solutions of the congruence 1.4, given by the relations 1.5. Therefore, the congruence 1.4 has $p - 1$ solutions. □

To go from 1.4 to 1.3, we distinguish the case when $p \equiv 1 \pmod{4}$ from the case when $p \equiv 3 \pmod{4}$ and prove the following.

Theorem 1.27. *There are $p + 1$ equivalent classes of proper solutions of the congruence $x^2 + y^2 + z^2 \equiv 0 \pmod{p}$.*

Proof. Case 1. $p \equiv 1 \pmod{4}$. In this case, -1 is quadratic residue of p , and so it exists an integer δ that verifies the congruence:

$$\delta^2 \equiv -1 \pmod{p}.$$

By the previous lemma, there are, modulo p , $p - 1$ solutions (a, b) of the equation:

$$1 + a^2 \equiv b^2 \Leftrightarrow 1 + a^2 + (\delta b)^2 \equiv 0 \pmod{p},$$

each of which correspond to the class $[1, a, \delta b]$.

We can also see that the congruence 1.2 can be verified by taking for z an integer divisible by p . In this case, neither x nor y can be divisible by p , otherwise we would have no longer a proper solution. For $z \equiv 0 \pmod{p}$ the congruence reduces to:

$$x^2 + y^2 \equiv 0 \pmod{p}.$$

As x and y are not divisible by p we have, modulo p , that $x^2 + y^2 = 0 \Leftrightarrow \left(\frac{x}{y}\right)^2 = -1$, which has two solutions, since -1 is a quadratic residue. Therefore, when $z = 0$, there are only two classes of proper solutions. These two classes of solutions joined to the $p - 1$ classes for which z is not divisible by p , giving us $p + 1$ classes of proper solutions of the congruence.

Case 2. $p \equiv 3 \pmod{4}$. In this case, -1 is not a quadratic residue of p , therefore is impossible that among the solutions of the congruence 1.4 there are solutions (a, b) for which the integer b is divisible by p . On the other hand, there are two solutions of the congruence 1.4, for which a is divisible by p , ($a \equiv 0, b \equiv \pm 1$), that are not solutions of the equation 1.2.

Since the congruence 1.4 has $p - 1$ solutions, if we put the two solutions, ($a \equiv 0, b \equiv \pm 1$), apart, we still have $p - 3$ solutions of this congruence. These $p - 3$ solutions break up into $\frac{p-3}{4}$ groups containing each four corresponding solutions $(\pm a, \pm b)$, since for each nonzero quadratic residue α , such that $1 + \alpha = \beta$ is again a quadratic residue, say $\alpha = a^2, \beta = b^2$, there correspond 4 solutions $(\pm a, \pm b)$ to the equation $1 + a^2 = b^2$. Conversely, every such 4 solutions correspond to a pair of quadratic residues α, β with $1 + \alpha = \beta$. Therefore, each of these groups represent one of the cases where for α , one of the $\frac{p-1}{2}$ quadratic residues, $1 + \alpha$ is again a quadratic residue.

Thus, for the other $\frac{p-1}{2} - \frac{p-3}{4} = \frac{p+1}{4}$ quadratic residues α' , we have that $1 + \alpha' = \beta'$ is a quadratic non-residue. Since α' is a quadratic quadratic residue, then $\alpha' = c^2$, for some $c \in \mathbb{F}_p$, and $(1 + c^2)(-1)$ is also a quadratic residue, since both factors are non-residues, so $\beta' = -d^2$, for some $d \in \mathbb{F}_p$. Therefore, each of the $\frac{p+1}{4}$ remaining residues corresponds to 4 solutions $(\pm c, \pm d)$ of the congruence:

$$1 + c^2 \equiv -d^2 \pmod{p},$$

which is equal to 1.2. Thus we have found $p + 1$ classes of solutions $[1, c, d]$, and it is clear that all solutions are obtained in this way.

Case 3. $p = 2$.

We have,

$$x^2 + y^2 + z^2 \equiv 0 \pmod{2},$$

and we see immediatly that that for this congruence there only three proper solutions.

$$\begin{cases} x \equiv 0, y \equiv 1, z \equiv 1 \\ x \equiv 1, y \equiv 0, z \equiv 1 \\ x \equiv 1, y \equiv 1, z \equiv 0 \end{cases} \pmod{2}.$$

□

Remark 1.28. For each proper solution of the equation $x^2 + y^2 + z^2 = 0$ over $\mathbb{F}_p$, we denote $\Xi = x + yi + zj$ its associated quaternion, over $\mathbb{F}_p$.

Proposition 1.29. *Let $P \in \mathcal{L}$ be a proper quaternion such that $p \mid N(P)$, for some prime p . Then, there exists a nonzero $\Xi = x + yi + zj$ over $\mathbb{F}_p$ such that $\Xi P \equiv 0 \pmod{p}$. We have $x^2 + y^2 + z^2 = 0$, and any two such solutions of $\Xi P = 0$ are equivalent if p is odd.*

Proof. Consider the proper quaternion $P = a + bi + cj + dk \in \mathcal{L}$ with norm $N(P)$, such that $N(P) = 0$ in $\mathbb{F}_p$. Since P is proper, not all a, b, c, d are divisible by p . In particular, we can always assume that a is not divisible by p because, if that was not the case, we could multiply P by an unit, u , in order to have a quaternion $P' = Pu$ with norm p such that its real part is not divisible by p , and $\Xi P' = 0$ implies that $\Xi P = 0$, modulo p . Thus, assume that $a \neq 0$ and let $\Xi = x + yi + zj$. Then, $\Xi P = 0$ is equivalent to the following system of equations:

$$\begin{cases} ax - by - cz \equiv 0 \\ bx + ay + dz \equiv 0 \\ cx - dy + az \equiv 0 \end{cases} \pmod{p}. \quad (1.7)$$

Note that we do not need to compare the fourth component of ΞP , since, from the system 1.7, if we multiply the first line by d , the second by c , the third by $-b$, divide all of them by a , and sum them, we arrive at the congruence:

$$dx + cy - bz \equiv 0 \pmod{p}, \quad (1.8)$$

and so this component yields no extra information. We can easily see that the determinant of the matrix associated with the system is $a(a^2 + b^2 + c^2 + d^2)$, which is 0 in $\mathbb{F}_p$, since $N(P) = 0$. Consider the cofactors of the system 1.7:

$$\begin{cases} a^2 + d^2; & +dc - ba; & -bd - ca; \\ dc + ba; & a^2 + c^2; & -cb + da; \\ -bd + ca; & -cb - da; & a^2 + b^2. \end{cases} \quad (1.9)$$

If all the three sums of squares that appear in the main diagonal are divisible by p , we will have that the sum of squares,

$$b^2 + c^2, \quad b^2 + d^2, \quad d^2 + c^2,$$

is divisible by p , since we have $a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{p}$. Therefore, the integers,

$$2a^2, \quad 2b^2, \quad 2c^2, \quad 2d^2,$$

will themselves be divisible by p . But if we assume that p is odd, the integers a, b, c, d would be divisible by p simultaneously, which is impossible. Therefore, at least one of the sums of squares must be nonzero, which implies that the rank of the coefficient matrix associated to the system 1.7 is precisely 2, since the determinant of the matrix associated with the system is 0. This means that the kernel of the matrix is 1-dimensional, i.e., that any two solutions of the congruence $\Xi P = 0 \pmod{p}$ are equivalent.

Now, if we sum the congruences in 1.7 multiplied, respectively, by x, y, z and remembering that a is not divisible by p we can deduce the congruence:

$$x^2 + y^2 + z^2 \equiv 0 \pmod{p} \quad (1.10)$$

□

From now on, we let $\Xi = x + yi + zj$ denote the unique class of quaternions over $\mathbb{F}_p$ associated with the equivalent class of solutions $x^2 + y^2 + z^2 = 0$, over $\mathbb{F}_p$.

Definition 1.30. Given a quaternion $P \in \mathcal{L}$ with $p \nmid P$ and $p \mid N(P)$, we say that P is of class Ξ if $\Xi \bar{P} = 0$.

Remark 1.31. If $\tilde{\Xi}$ is any lift of Ξ in $\mathcal{L}$, i.e., if $\tilde{\Xi} \in \mathcal{L}$ is such that the reduction modulo p is Ξ , then $\tilde{\Xi}$ is of class Ξ .

Proposition 1.32. *Let p be an odd prime. For every P of class Ξ , there exists P_0 of class Ξ such that $N(P_0) = p$. Furthermore, any prime quaternion P of class Ξ is of the form uP_0 where u is a unit.*

We follow the proof of Proposition 7 in [Per11].

Proof. Consider a fixed lift $\tilde{\Xi}$ of Ξ . From Theorem 1.20 and Lemma 1.21, exists a factorization of $\tilde{\Xi} = Q_0 P_0$, where $Q_0, P_0 \in \mathcal{L}$ and $N(P_0) = p$. By the same results, there exists a factorization of $P = Q_1 P_1$, where $N(P_1) = p$. Since P is of class Ξ , one has $p \mid \tilde{\Xi} \bar{P}$, i.e., $p \mid Q_0 P_0 \bar{P}_1 \bar{Q}_1$. By Lemma 1.25, since $p \nmid Q_0 P_0$, we have $p \mid P_0 \bar{P}_1 \bar{Q}_1$. The same argument, shows that we have $p \mid P_0 \bar{P}_1$. Therefore, $P_1 = u P_0$, where u is a unit. If P is irreducible, then $P = Q_1 P_1$ with Q_1 a unit. Thus, P is of the form $u' P_0$, where $u' = Q_1 u$ is a unit.

It remains to see that our result does not depend on the lifting. Let $\Xi_1 = \alpha \Xi$, with nonzero $\alpha \in \mathbb{F}_p$, be any other representative in the same equivalent class of Ξ . It is not hard to see that any lifting $\tilde{\Xi}_1$ of Ξ_1 is related to Ξ by the relation:

$$\tilde{\Xi}_1 = a \Xi_1 + pQ$$

where a is an integer not divisible by p such that $a \equiv \alpha \pmod{p}$, and Q is in $\mathcal{L}$. Thus, one has:

$$\tilde{\Xi}_1 = a \Xi_1 + pQ = a(Q_0 P_0) + Q \bar{P}_0 P_0 = (aQ_0 + Q \bar{P}_0) P_0$$

which shows that uP_0 is well-defined as a common irreducible right divisor for all lifts of members in the class Ξ . □

Under the condition that p is odd, recall that, from Theorem 1.27, we have $p + 1$ equivalent classes of Ξ . Suppose that for each of these classes we choose a representative. Then, by Proposition 1.32, we can associate each of these classes to a well defined class of prime element of the form uP_0 , if we call this association Ψ , then Ψ must be injective. For instance, suppose that $\Psi(\Xi_1) = \Psi(\Xi_2)$ that is equal to class of uP_0 . This means we have, modulo p , $\Xi_1 \bar{uP_0} = \Xi_2 \bar{uP_0} = 0$, therefore, by Proposition 1.29, Ξ_1 and Ξ_2 are equivalent.

The map Ψ is surjective, since if we define a mapping ψ from the class of uP_0 to the class of Ξ by sending $\psi(uP_0)$ to the class Ξ defined by the condition that $\Xi\bar{P}_0 = 0$, it is easy to see that Ψ and ψ are inverses of each other. Hence Ψ is a bijection.

Corollary 1.33. *Let $p \in \mathbb{Z}$ be a prime. There are $p + 1$ Lipschitz primes up to associates that lie above p .*

Proof. The case when p is odd follows from everything we have discussed above. If $p = 2$, then it is straightforward to check directly that, for any $u \in \mathcal{L}^*$, $u(1 + i)$, $u(1 + j)$, and $u(1 + k)$ are not equivalent. $\square$

Using this corollary we prove a similar result in the Hurwitz integers. For that consider the following lemma.

Lemma 1.34. *Let $\alpha = a + bi + cj + dk \in \mathcal{L}$ be such that $N(\alpha) \equiv 1 \pmod{2}$. Then, one has $\forall u \in \mathcal{H}^* \setminus \mathcal{L}^*, u\alpha \in \mathcal{H} \setminus \mathcal{L}$.*

Proof. We have $1 \equiv N(\alpha) \equiv a^2 + b^2 + c^2 + d^2 \equiv a + b + c + d \equiv \pm a \pm b \pm c \pm d \pmod{2}$. Using the explicit expression 1.1, we have that the coefficients of $(\pm 1 \pm i \pm j \pm k)\alpha$ are all of the form $\pm a \pm b \pm c \pm d$, thus they are all odd. Now, if $u \in \mathcal{H}^* \setminus \mathcal{L}^*$, we have that u is of the form $u = \frac{(\pm 1 \pm i \pm j \pm k)}{2}$, so $u\alpha = \frac{1}{2}(\pm 1 \pm i \pm j \pm k)\alpha \in \mathcal{H} \setminus \mathcal{L}$. $\square$

From Corollary 1.33, there are only $p + 1$ Lipschitz primes up to left associates that lie above p . If we consider Hurwitz primes, it follows from the Lemma 1.34 and Proposition 1.24 that the number of classes must be the same when p is odd. If $p = 2$, then there is only one Hurwitz prime above p , since, for example, $u = \frac{1}{2}(1 + i + j + k)$ implies that $u(1 + i) = (i + j)$, and $u(i + j) = 1 + k$. Thus, we have the following:

Corollary 1.35. *Let p be a rational prime. If p is odd, there are $p + 1$ Hurwitz primes up to left multiplication by units that lie above p . If $p = 2$, then there is only one prime up to associates.*

Definition 1.36. We denote by Π_p the set consisting of the Hurwitz primes that lie above p , up to unit multiplication.

1.2 Finite fields

Since we will work mainly in the field $\mathbb{F}_p$, it is important to gather some notions and results about the theory of finite fields. The main objective of this section is to recall some well known facts, in particular those related to field extensions, and introduce the concept of cyclotomic fields as well as some results that will be fulcral to the proof of Theorem 3.7 in Chapter 3. We follow mainly [LN96], [Ser73], [IR90].

1.2.1 Generalities and field extensions

In this section, our main purpose is to recall some general notions about fields and fields extensions, this is fundamental to understand the structure of field fields in section 1.2.2. All the results are present in Chapter 1, Section 3 and 4 of [LN96]. The first notion we want to recall is the characteristic of a finite field. To do that, we first recall its general definition.

Definition 1.37. Let R be an arbitrary ring (with unity). Let g be the unique homomorphism from $\mathbb{Z}$ to R . The **characteristic** of R is the natural number n such that $\ker(g) = n\mathbb{Z}$.

Remark 1.38. From the above definition follows that the characteristic of R is the natural number n such that R contains a subring isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Theorem 1.39. A ring $R \neq \{0\}$ of positive characteristic having no zero divisors must have prime characteristic.

Proof. Since R contains no zero divisors, $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to a subring of R with no zero divisors. Therefore, itself must have no zero divisors, which only happens when n is prime or 0, but since the characteristic of R is positive, n must be prime. $\square$

Corollary 1.40. A finite field has prime characteristic.

Recall that, for an arbitrary ring R , a polynomial over R is an expression of the form

$$f(x) = \sum_{i=0}^n a_i x^i = a_0 + a_1 x + \cdots + a_n x^n, \quad (1.11)$$

where n is not negative and the coefficients a_i belong to R . The ring formed by the polynomials over R with the usual operations is called the polynomial ring over R and denoted by $R[x]$. If the polynomial f in 1.11 is not zero, we can suppose $a_n \neq 0$. Then $a_n \neq 0$ is called the **leading coefficient** of $f(x)$, while n is called the **degree** of $f(x)$, and denoted $\deg(f) = n$.

Recall that if $\mathbb{F}$ is a field then $\mathbb{F}[x]$ is a principal ideal domain and that for every ideal $J \neq 0$ of $\mathbb{F}[x]$ exists an uniquely determined monic polynomial g with $J = \langle g \rangle = \{f(x)g(x) : f(x) \in \mathbb{F}[x]\}$. For more detail see Theorem 1.54 of [LN96].

The next concept is fundamental to understand field extensions.

Definition 1.41. A polynomial $p \in \mathbb{F}[x]$ is said to be **irreducible** in $\mathbb{F}[x]$ if p has positive degree and $p = bc$ implies that either b or c is a constant polynomial.

We say that an element $b \in \mathbb{F}$ is a **root** of a polynomial $f \in \mathbb{F}[x]$, if $f(b) = 0$, and the **multiplicity** k of b is the positive integer such that $(x - b)^k$ divides $f(x)$ but $(x - b)^{k+1}$ does not. Also b is a root of f if and only if $x - b$ divides $f(x)$.

Theorem 1.42. Let $f \in \mathbb{F}[x]$ with non negative degree n . If $b_1, \dots, b_m \in \mathbb{F}$ are distinct roots of f with multiplicities $k_1, \dots, k_m$, respectively, then $(x - b_1)^{k_1} \cdots (x - b_m)^{k_m}$ divides $f(x)$. Consequently, $k_1 + \cdots + k_m \leq n$, and f can have at most n distinct roots in $\mathbb{F}$.

Definition 1.43. If $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$, then the derivate f' of f is defined by $f' = f'(x) = a_1 + 2a_2 x + \cdots + na_n x^{n-1}$.

Theorem 1.44. *The element $b \in \mathbb{F}$ is a multiple root of $f \in \mathbb{F}[x]$ if and only if it is a root of both f and f' .*

If $\mathbb{F}$ is a field, then a subset $\mathbb{K}$ of $\mathbb{F}$ that is itself a field under the operation of $\mathbb{F}$ is a subfield of $\mathbb{F}$. In this context, $\mathbb{F}$ is called an **extension** of $\mathbb{K}$. If $\mathbb{K} \neq \mathbb{F}$, $\mathbb{K}$ is a proper subfield of $\mathbb{F}$.

Definition 1.45. A field containing no proper subfield is called a **prime field**.

The intersection of any nonempty subfields of a given field $\mathbb{F}$ is again a subfield. Thus, if we form the intersection of all subfields of $\mathbb{F}$, we obtain a subfield of $\mathbb{F}$ with no proper subfields, and we call it **the prime subfield of $\mathbb{F}$** .

Theorem 1.46. *The prime subfield of a field $\mathbb{F}$ is isomorphic to either $\mathbb{F}_p$ or $\mathbb{Q}$, according as the characteristic of $\mathbb{F}$ is a prime or 0.*

Definition 1.47. Let $\mathbb{K}$ be a subfield of the field $\mathbb{F}$ and M any subset of F . Then the field $\mathbb{K}(M)$ is defined as the intersection of all subfields of $\mathbb{F}$ containing both $\mathbb{K}$, and M and is called the extension (field) of $\mathbb{K}$ obtained by adjoining the elements in M . For a finite set $M = \{\theta_1, \dots, \theta_n\}$ we write $\mathbb{K}(M) = \mathbb{K}(\theta_1, \dots, \theta_n)$. If M consists of a single element $\theta \in \mathbb{F}$, then $L = \mathbb{K}(\theta)$ is said to be a simple extension of $\mathbb{K}$, and θ is called a defining element of L over $\mathbb{K}$.

The way $\mathbb{K}(M)$ is defined makes it the smallest subfield of $\mathbb{F}$ containing both $\mathbb{K}$ and M .

Definition 1.48. Let $\mathbb{K}$ be a subfield of $\mathbb{F}$ and $\theta \in \mathbb{F}$. If θ satisfies a nontrivial polynomial equation with coefficients in $\mathbb{K}$, that is, if $a_n\theta^n + \dots + a_1\theta + a_0 = 0$, with $a_i \in \mathbb{K}$, not all 0, then θ is said to be **algebraic** over $\mathbb{K}$. An extension $\mathbb{L}$ of $\mathbb{K}$ is called algebraic over $\mathbb{K}$ if every element of $\mathbb{L}$ is algebraic over $\mathbb{K}$.

Let $\theta \in \mathbb{F}$ be algebraic over $\mathbb{K}$ and consider the set $J = \{f \in \mathbb{K}[x] : f(\theta) = 0\}$. It is easily checked that J is an ideal of $\mathbb{K}[x]$, and since $\mathbb{K}[x]$ is a principal ideal domain, there is a uniquely determined monic polynomial g such that $J = \langle g \rangle$. In fact, we also have that g is irreducible in $\mathbb{K}[x]$, because since g has the root θ , if $g = h_1h_2$, with $\deg(h_i) < \deg(g)$ then θ would also be a root of h_1 or h_2 , and either h_1 or h_2 is in J , and so is divisible by g , which is not possible.

Definition 1.49. If $\theta \in \mathbb{F}$ is algebraic over $\mathbb{K}$, then the unique monic polynomial $g \in \mathbb{K}[x]$ generating the ideal $J = \{f \in \mathbb{K}[x] : f(\theta) = 0\}$ of $\mathbb{K}[x]$ is called the **minimal polynomial** of θ over $\mathbb{K}$.

Theorem 1.50. *If $\theta \in \mathbb{F}$ is algebraic over $\mathbb{K}$, then its minimal polynomial g over $\mathbb{K}$ has the following properties:*

1. g is irreducible in $\mathbb{K}[x]$.
2. For $f \in \mathbb{K}[x]$ we have $f(\theta) = 0$ if and only if g divides f .
3. g is the monic polynomial in $\mathbb{K}[x]$ of the least degree having θ as a root.

Proof. The first property was already noted and the second follows from the definition of g . For the last property, just note that any monic polynomial in $\mathbb{K}[x]$ having θ as a root must be a multiple of g , so its degree is equal to that of g or it is larger. $\square$

If $\mathbb{L}$ is an extension field of $\mathbb{K}$, then $\mathbb{L}$ may be viewed as a vector space over $\mathbb{K}$, since the elements of $\mathbb{L}$ form an Abelian group, and if $k \in \mathbb{K}$ and $\ell \in \mathbb{L}$ then $k\ell \in \mathbb{L}$ and all the required laws of multiplication by scalars are satisfied.

Definition 1.51. Let $\mathbb{L}$ be an extension field of $\mathbb{K}$. If $\mathbb{L}$, considered as a vector space over $\mathbb{K}$, is finite-dimensional, then $\mathbb{L}$ is called a **finite extension** of $\mathbb{K}$. The dimension of the vector space $\mathbb{L}$ over $\mathbb{K}$ is then called the **degree of $\mathbb{L}$ over $\mathbb{K}$** , $[\mathbb{L} : \mathbb{K}]$.

Theorem 1.52. *Every finite extension of $\mathbb{K}$ is algebraic over $\mathbb{K}$.*

Proof. Let $\mathbb{L}$ be a finite extension of $\mathbb{K}$ and put $[\mathbb{L} : \mathbb{K}] = m$. For $\theta \in \mathbb{L}$, the $m + 1$ elements $1, \theta, \dots, \theta^m$ must be linearly dependent over $\mathbb{K}$, and so we get a relation $a_0 + a_1\theta + \dots + a_m\theta^m = 0$ with $a_i \in \mathbb{K}$ not all being zero. This is simply saying that θ is algebraic over $\mathbb{K}$. $\square$

If we consider the simple extension $\mathbb{K}(\theta)$ of $\mathbb{K}$, where $\theta \in \mathbb{F}$ is algebraic over $\mathbb{K}$ and $\mathbb{F}$ is an extension of $\mathbb{K}$, we get that $\mathbb{K}(\theta)$ is a finite extension of $\mathbb{K}$.

Theorem 1.53. *Let $\theta \in \mathbb{F}$ be algebraic of degree n over $\mathbb{K}$ and let g be the minimal polynomial of θ over $\mathbb{K}$. Then:*

1. $\mathbb{K}(\theta)$ is isomorphic to $\mathbb{K}[x]/\langle g \rangle$.
2. $[\mathbb{K}(\theta) : \mathbb{K}] = n$ and $\{1, \theta, \dots, \theta^{n-1}\}$ is a basis of $\mathbb{K}(\theta)$ over $\mathbb{K}$.
3. Every $\alpha \in \mathbb{K}(\theta)$ is algebraic over $\mathbb{K}$ and its degree over $\mathbb{K}$ is a divisor of n .

Proof. See the proof of Theorem 1.86 in [LN96]. $\square$

It is important to notice that the elements of the simple algebraic extension $\mathbb{K}(\theta)$ of $\mathbb{K}$ are polynomial expressions in θ . In fact, any element of $\mathbb{K}(\theta)$ can be uniquely represented in the form $a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}$, with $a_i \in \mathbb{K}$.

The last theorem works under the assumption that both $\mathbb{K}$ and θ are embedded in a larger field F . One would also want to construct a simple algebraic extension without the reference to a previously given larger field. For that, consider:

Theorem 1.54. *Let $f \in \mathbb{K}[x]$ be irreducible over the field $\mathbb{K}$. Then exists a simple algebraic extension of $\mathbb{K}$ with a root of f as a defining element.*

Proof. See proof of Theorem 1.87 in [LN96]. $\square$

The following theorem is easily obtained.

Theorem 1.55. *Let α and β be two roots of the polynomial $f \in \mathbb{K}[x]$ that is irreducible over $\mathbb{K}$. Then $\mathbb{K}(\alpha)$ and $\mathbb{K}(\beta)$ are isomorphic under an isomorphism mapping α to β and keeping the elements of $\mathbb{K}$ fixed.*

If we want to find an extension field that contains all roots of a given polynomial we are motivated to define:

Definition 1.56. Let $f \in \mathbb{K}[x]$ be of positive degree and $\mathbb{F}$ an extension field of $\mathbb{K}$. Then f is said to **split** in $\mathbb{F}$ if f can be written as a product of linear factors in $\mathbb{F}[x]$ - that is, if there exist elements $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{K}$ such that

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

where a is the leading coefficient of f . The field F is a splitting field of f over $\mathbb{K}$ if f splits in $\mathbb{F}$ and if $\mathbb{F} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$.

The next theorem is important since it allows us to speak of the splitting field of f over $\mathbb{K}$. It is obtained from $\mathbb{K}$ by adjoining finitely many algebraic elements over $\mathbb{K}$.

Theorem 1.57 (Existence and Uniqueness of Splitting Field). *If $\mathbb{K}$ is a field and f any polynomial of positive degree in $\mathbb{K}[x]$, then there exists a splitting field of f over $\mathbb{K}$. Any two splitting fields of f over $\mathbb{K}$ are isomorphic under an isomorphism which keeps the elements of $\mathbb{K}$ fixed and maps roots of f into each other.*

Definition 1.58. Let $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{K}[x]$ and $g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m \in \mathbb{K}[x]$ be two polynomials of formal degree n and m , respectively. Then the resultant $R(f, g)$ of the two polynomials is defined by the determinant

$$R(f, g) = \begin{vmatrix} a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_n \\ b_0 & b_1 & \cdots & & b_m & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & & b_m & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_m \end{vmatrix},$$

of order $m + n$.

If $\deg(f) = n$ and $f(x) = a_0(x - \alpha_1) \cdots (x - \alpha_n)$ in the splitting field of f over $\mathbb{K}$, then $R(f, g)$ is also given by the formula:

$$R(f, g) = a_0^m \prod_{i=1}^n g(\alpha_i).$$

Remark 1.59. In this case, $R(f, g) = 0$ if and only if f and g have a common root, which is the same as saying that f and g have a common divisor in $\mathbb{K}[x]$ of positive degree.

1.2.2 Structure of finite fields

The constructions we made in the previous section are useful to get a better understanding of the structure of finite fields. The results of this section follow the work of Chapter 2, Section 1 and 2 of [LN96].

Lemma 1.60. *Let $\mathbb{F}$ be a finite field containing a subfield $\mathbb{K}$ with q elements. Then $\mathbb{F}$ has q^m elements, where $m = [\mathbb{F} : \mathbb{K}]$.*

Proof. Since $\mathbb{F}$ is a vector space over $\mathbb{K}$, and is finite, it is finite dimensional as a vector space over $\mathbb{K}$. If $[\mathbb{F} : \mathbb{K}] = m$, then $\mathbb{F}$ has a basis over $\mathbb{K}$ consisting of m elements, $b_1, b_2, \dots, b_m$. Thus, every element of $\mathbb{F}$ can be uniquely represented in the form $a_1 b_1 + \dots + a_m b_m$, where $a_1, \dots, a_m \in \mathbb{K}$. Since each a_i can have q values, $\mathbb{F}$ has exactly q^m elements. $\square$

The next theorem is adapted from Theorem 2.2 in [LN96].

Theorem 1.61. *Let $\mathbb{F}$ be a finite field. Then $\mathbb{F}$ has p^n elements, where the prime p is the characteristic of $\mathbb{F}$ and n is the degree of $\mathbb{F}$ over its prime subfield.*

Proof. Since $\mathbb{F}$ is finite, its characteristic is a prime p according to Corollary 1.40. Therefore, the prime subfield K is isomorphic to $\mathbb{F}_p$ by Theorem 1.46 and thus contains p elements. The rest follows from the previous lemma. $\square$

We would like to construct a finite field with p^n elements starting with $\mathbb{F}_p$, for every prime p and $n \in \mathbb{N}$. Thus we use following results

Lemma 1.62. *If $\mathbb{F}$ is a finite field with q elements, then every $a \in \mathbb{F}$ satisfies $a^q = a$.*

Proof. The identity $a^q = a$ is trivial for $a = 0$. On the other hand, the nonzero element of F form a group of order $q - 1$ under multiplication. Thus $a^{q-1} = 1$ for all $a \in \mathbb{F}$, with $a \neq 0$, and multiplication by a yields the desired result. $\square$

Lemma 1.63. *If $\mathbb{F}$ is a finite field with q elements and $\mathbb{K}$ is a subfield of $\mathbb{F}$, then the polynomial $x^q - x$ in $\mathbb{K}[x]$ factors in $\mathbb{F}[x]$ as*

$$x^q - x = \prod_{a \in \mathbb{F}} (x - a) \quad (1.12)$$

and $\mathbb{F}$ is a splitting field of $x^q - x$ over $\mathbb{K}$.

Proof. The polynomial $x^q - x$ of degree q has at most q roots in $\mathbb{F}$. By the previous lemma, we know that these q roots are precisely all the elements of $\mathbb{F}$. Therefore, $x^q - x$ splits in $\mathbb{F}$ as stated, and it cannot split in any smaller field. $\square$

Theorem 1.64 (Existence and Uniqueness of Finite fields). *For every prime p and every positive integer n exists a finite field with p^n elements. Any field with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x$.*

This theorem and its proof are essentially Theorem 2.5 of [LN96].

Proof. (Existence) For $q = p^n$ consider $x^q - x$ in $\mathbb{F}_p[x]$, and let $\mathbb{F}$ be its splitting field over $\mathbb{F}_p$. This polynomial has q distinct roots in F , since its derivative is $qx^{q-1} - 1 = -1$ and so it cannot have no common roots with $x^q - x$ (compare with Theorem 1.44). Let $S = \{a \in F : a^q - a = 0\}$. Then, it is easy to see that S is a subfield of $\mathbb{F}$. But, on the other hand, $x^q - x$ must split in S , since S contains all its roots. Thus $\mathbb{F} = S$, and since S has q elements, $\mathbb{F}$ is a finite field with q elements.

(Uniqueness) Let $\mathbb{F}$ be a finite field with $q = p^n$ elements. Then $\mathbb{F}$ has characteristic p by Theorem 1.61 and so contains $\mathbb{F}_p$ as a subfield. It follows from the previous lemma that $\mathbb{F}$ is a splitting field of $x^q - x$ over $\mathbb{F}_p$. Thus, the desired result is a consequence of the uniqueness of splitting field, which was noted in Theorem 1.57. $\square$

The uniqueness part of the theorem allows us to speak of the finite field with $q = p^n$ elements and denote it $\mathbb{F}_q$.

The following theorem and its proof can be seen in Theorem 2.8 of [LN96].

Theorem 1.65. *For every finite field $\mathbb{F}_q$ the multiplicative group $\mathbb{F}_q^\times$ of nonzero elements of $\mathbb{F}_q$ is cyclic.*

Proof. We can assume $q \geq 3$. Let $h = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ be the prime factor decomposition of the order $h = q - 1$ of the group $\mathbb{F}_q^\times$. For every i , $1 \leq i \leq m$, the polynomial $x^{h/p_i} - 1$ has at most h/p_i roots in $\mathbb{F}_q$. Since $h/p_i < h$, it follows that there are nonzero elements in $\mathbb{F}_q$ that are not roots of this polynomial. Let a_i be such an element and set $b_i = a_i^{h/p_i^{r_i}}$. We have $b_i^{p_i^{r_i}} = 1$, hence the order of b_i is a divisor of $p_i^{r_i}$ and is therefore of the form $p_i^{s_i}$ with $0 \leq s_i \leq r_i$. On the other hand,

$$b_i^{p_i^{r_i} - 1} = a_i^{h/p_i} \neq 1,$$

and so the order of b_i is $p_i^{r_i}$. We claim that the element $b = b_1 b_2 \cdots b_m$ has order h . Suppose, on the contrary, that the order of b is a proper divisor of h and is therefore a divisor of at least one of the m integers h/p_i , $1 \leq i \leq m$, say of h/p_1 . Then we have

$$1 = b^{h/p_1} = b_1^{h/p_1} b_2^{h/p_1} \cdots b_m^{h/p_1}.$$

Now if $2 \leq i \leq m$, then $p_i^{r_i}$ divides h/p_1 , and hence $b_i^{h/p_1} = 1$. Therefore $b_1^{h/p_1} = 1$. This implies that the order of b_1 must divide h/p_1 , which is impossible since the order of b_1 is $p_1^{r_1}$. Thus, $\mathbb{F}_q^\times$ is a cyclic group with generator b . $\square$

Definition 1.66. A generator of the cyclic group $\mathbb{F}_q^\times$ is called a **primitive element** of $\mathbb{F}_q$.

It is a well-known result that a finite cyclic group of order m contains $\phi(m)$ generators, this follows from the fact that there are precisely $\phi(m)$ elements of order m .

Theorem 1.67. *Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_r$ a finite extension field. Then $\mathbb{F}_r$ is a simple algebraic extension of $\mathbb{F}_q$ and every primitive element of $\mathbb{F}_r$ can serve as a defining element of $\mathbb{F}_r$ over $\mathbb{F}_q$.*

Proof. Let ξ be a primitive element of $\mathbb{F}_r$. We clearly have $\mathbb{F}_q(\xi) \subseteq \mathbb{F}_r$. On the other hand, $\mathbb{F}_q(\xi)$ contains 0 and all powers of ξ , and so all elements of $\mathbb{F}_r = \mathbb{F}_q(\xi)$. $\square$

Corollary 1.68. *For every finite field $\mathbb{F}_q$ and every positive integer n there exist an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n .*

The last thing we need is to recall the following two definitions of trace and norm.

Definition 1.69. For $\alpha \in \mathbb{F} = \mathbb{F}_{q^m}$ and $\mathbb{K} = \mathbb{F}_q$, the trace $\text{Tr}_{\mathbb{F}/\mathbb{K}}(\alpha)$ of α over $\mathbb{K}$ is defined by

$$\text{Tr}_{\mathbb{F}/\mathbb{K}}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.$$

The norm $N_{\mathbb{F}/\mathbb{K}}(\alpha)$ of α over $\mathbb{K}$ is:

$$N_{\mathbb{F}/\mathbb{K}}(\alpha) = \alpha \cdot \alpha^q \cdots \alpha^{q^{m-1}} = \alpha^{(q^m-1)/(q-1)}.$$

Remark 1.70. The previous definition follow from the fact that, if we view $\mathbb{F}$ as a Galois extension of $\mathbb{K}$, then the trace $\text{Tr}_{\mathbb{F}/\mathbb{K}}(\alpha)$ and norm $N_{\mathbb{F}/\mathbb{K}}$ are simply the sum and multiplication of all the conjugates of α , since the automorphism of Frobenius is a generator of this galois group.

1.2.3 Cyclotomic polynomials

We now introduce some general theory about cyclotomic polynomials, present in Section 3 of [LN96]. For that, let n be a positive integer. The splitting field of $x^n - 1$ over a field $\mathbb{K}$ is called the n^{th} **cyclotomic field** over $\mathbb{K}$ and is denoted by $\mathbb{K}^{(n)}$. The roots of $x^n - 1$ in $\mathbb{K}^{(n)}$ are called the n^{th} **roots of unity** over $\mathbb{K}$ and the set of all these roots is denoted by $E^{(n)}$.

Theorem 1.71. *Let n be a positive integer and $\mathbb{K}$ a field of characteristic p . Then:*

1. *If p does not divide n , $E^{(n)}$ is a cyclic group of order n with respect to multiplication in $\mathbb{K}^{(n)}$.*
2. *If p divides n , write $n = mp^e$ with positive integers m and e and m not divisible by p . Then $\mathbb{K}^{(n)} = \mathbb{K}^{(m)}$, $E^{(n)} = E^{(m)}$, and the roots of $x^n - 1$ in $\mathbb{K}^{(n)}$ are the m elements of $E^{(m)}$, each attained with multiplicity p^e .*

We follow the proof of Theorem 2.42 in [LN96].

Proof. For the first claim: The case $n = 1$ is trivial. For $n \geq 2$, $x^n - 1$ and its derivation nx^{n-1} have no roots in common, since 0 is the only root of nx^{n-1} in $\mathbb{K}^n$. Therefore, by Theorem 1.44, $x^n - 1$ cannot have multiple roots, so $E^{(n)}$ has n elements. Now, if $\alpha, \beta \in E^{(n)}$, then $(\alpha\beta^{-1})^n = \alpha^n(\beta^n)^{-1} = 1$, thus $\alpha\beta^{-1} \in E^{(n)}$. So, E^n is a multiplicative group. Let $n = p_1^{e_1} \cdots p_s^{e_s}$ be the prime factor decomposition of n . Then one shows, by the same argument as in the proof of Theorem 1.65, that for each i , there exists an element $\alpha_i \in E^{(n)}$ that is not a root of the polynomial $x^{n/p_i} - 1$, that $\beta = \alpha^{n/p_i^{e_i}}$ has order $p_i^{e_i}$ and that $E^{(n)}$ is a cyclic group with generator $\beta = \beta_1 \cdots \beta_s$.

The second claim follows immediately from $x^n - 1 = x^{mp^e} - 1 = (x^m - 1)^{p^e}$ and the first part. $\square$

Definition 1.72. Let $\mathbb{K}$ be a field of characteristic p and n a positive integer not divisible by p . Then, a generator of the cyclic group $E^{(n)}$ is called a **primitive** n^{th} root of unity over $\mathbb{K}$.

We know that under the conditions of the last definition there are exactly $\phi(n)$ different primitive n^{th} roots of unity over $\mathbb{K}$. If ξ is one of them, then all primitive n^{th} roots of unity over $\mathbb{K}$ are given by ξ^s , where $1 \leq s \leq n$ and $\gcd(s, n) = 1$. The polynomial whose roots are precisely the n^{th} roots of the unity over k are exactly what we have been building up to.

Definition 1.73. Let $\mathbb{K}$ be a field of characteristic p , n a positive integer not divisible by p and ξ a primitive n^{th} root of unity over $\mathbb{K}$. Then the polynomial

$$\Phi_n(x) = \prod_{\substack{s=1 \\ \gcd(s,n)=1}}^n (x - \xi^s) \quad (1.13)$$

is called the n^{th} **cyclotomic polynomial** over $\mathbb{K}$.

Remark 1.74. If $\mathbb{K} = \mathbb{F}_p$ and $n = p$, we define $\Phi_p(x)$ as $(x - 1)^{p-1}$.

The polynomial $\Phi_n(x)$ is independent of the choice of ξ , has degree $\phi(n)$ and its coefficients obviously belong to the n^{th} cyclotomic field over $\mathbb{K}$. In fact, they are in the prime subfield of $\mathbb{K}$.

Theorem 1.75. Let $\mathbb{K}$ be a field of characteristic p and n a positive integer not divisible by p . Then:

1. $x^n - 1 = \prod_{d|n} \Phi_d(x)$;
2. the coefficients of $\Phi_n(x)$ belong to the prime subfield of $\mathbb{K}$.

We follow the proof of Theorem 2.45 in [LN96].

Proof. For the first claim: consider that each n^{th} root of the unity over $\mathbb{K}$ is a primitive d^{th} root of unity over $\mathbb{K}$ for exactly one positive divisor d of n . In detail, if ξ is a primitive n^{th} root of the unity and ξ^s is an arbitrary n^{th} root of the unity over $\mathbb{K}$, then $d = n / \gcd(s, n)$, which means that d is the order of ξ^s in $E^{(n)}$. Since

$$x^n - 1 = \prod_{s=1}^n (x - \xi^s),$$

the formula is obtained by collecting those factors $(x - \xi^s)$ for which ξ^s is a primitive d^{th} root of the unity over k .

The second claim is proved by induction on n . Note that $\Phi_n(x)$ is a monic polynomial. For $n = 1$ we have $\Phi_1 = (x - 1)$ and the claim is valid. Now, let $n > 1$ and suppose is true for all $\Phi_d(x)$ with $1 \leq d < n$. Then we have by the first part that $\Phi_n(x) = (x^n - 1)/f(x)$, where $f(x) = \prod_{d|n, d < n} \Phi_d(x)$. The induction hypothesis implies that $f(x)$ is a polynomial with coefficients in the prime subfield of $\mathbb{K}$. Using long division with $x^n - 1$ and the monic polynomial $f(x)$, we see that the coefficients of $\Phi_n(x)$ belong to the prime subfield of $\mathbb{K}$. $\square$

1.3 Quadratic forms

In this section, we give some elementary notions about quadratic forms and, in particular, we outline the theory of quadratic forms over finite fields. Throughout this section we follow mainly Chapter 4 of [Ser73]. We also use results present in [Shi10].

Definition 1.76. Let V be a module over a commutative ring R . A mapping $q : V \times V \rightarrow R$ satisfying the following conditions:

1. $q(x, y) = q(y, x)$,
2. $q(rx + sy, z) = rq(x, z) + sq(y, z)$, for $r, s \in R$ and $x, y, z \in V$,

is called a **symmetric bilinear form** and the pair (V, q) is a **symmetric bilinear module** over R . When R is a field we often use *space* instead of *module*.

Definition 1.77. Let V be a module over a commutative ring R . A function $Q : V \rightarrow R$ is called a **quadratic form** on V if:

1. $Q(ax) = a^2Q(x)$ for $a \in R$ and $x \in V$,
2. $q(x, y) := Q(x + y) - Q(x) - Q(y)$ is a symmetric bilinear form.

The pair (V, Q) is called a **quadratic module** and q is the associated symmetric bilinear form.

We limit ourselves to the case where R is a field $\mathbb{K}$ of characteristic different from 2, thus the R -module V is then a $\mathbb{K}$ -vector space, which we suppose has finite dimension. If we let,

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

then $Q(x) = x \cdot x$. Conversely, for a symmetric bilinear form $x \cdot y$, if $Q(x) = x \cdot x$, then we have a quadratic form such that $Q(x + y) - Q(x) - Q(y) = 2x \cdot y$, thus exists a bijective correspondence between quadratic forms and symmetric bilinear forms.

Definition 1.78. The map $(x, y) \mapsto x \cdot y$ is called the **scalar product** associated with Q .

Given a basis $(e_i)_{1 \leq i \leq n}$ of V , the matrix of Q with respect to this basis is the matrix $A = (a_{ij})$ where $a_{ij} = e_i \cdot e_j$. If $x = \sum x_i e_i$ is an element of V , then:

$$Q(x) = \sum a_{ij} x_i x_j = x^t A x,$$

which shows that $Q(x)$ is a quadratic form in $x_1, \dots, x_n$ in the usual sense, from Linear Algebra.

For another basis $(v_i)_{1 \leq i \leq n}$, there is an invertible matrix B , such that $(v_1, \dots, v_n) = (e_1, \dots, e_n)B$. The matrix A' of Q with respect to the new basis is then $A' = B^t A B$. In particular,

$$\det(A') = \det(A) \det(B)^2,$$

which shows that $\det(A)$ is determined up to multiplication by an element of $\mathbb{K}^{\times 2}$.

Definition 1.79. The **discriminant** of a quadratic form Q , denoted by $\text{disc}(Q)$, is the class $\det(A)\mathbb{K}^{\times 2}$ in $\mathbb{K}^{\times}/\mathbb{K}^{\times 2}$, where A is the matrix defined above.

Definition 1.80. Let (V, Q) be a quadratic module over $\mathbb{K}$. Two elements $x, y \in V$ are called orthogonal if $x \cdot y = 0$.

Two subsets X and Y are said to be orthogonal if $x \cdot y = 0$ for all $x \in X$ and $y \in Y$.

Definition 1.81. For a subset X of V , the **orthogonal complement** of X in V is the set:

$$X^\perp = \{v \in V : v \cdot x = 0 \text{ for all } x \in X\}.$$

The orthogonal complement of V is called the **radical** of V and is denoted by $\text{rad}(V)$. If $\text{rad}(V) = 0$ we say that Q is **nondegenerate**. Let (V, Q) be a quadratic module over $\mathbb{K}$, and V^* be the dual space of V . The function $b : V \rightarrow V^*$ defined by:

$$\begin{aligned} b : V &\rightarrow V^* \\ x &\mapsto b_x \end{aligned}$$

such that

$$\begin{aligned} b_x : V &\rightarrow V \\ y &\mapsto x \cdot y \end{aligned}$$

is clearly linear, and its kernel is precisely $\text{rad}(V)$. Thus, Q is nondegenerate if and only if b is an isomorphism. Notice that, if we have a basis $(v_i)_{1 \leq i \leq n}$ of V , then $(v_i^*)_{1 \leq i \leq n}$ is a basis of V^* , where (v_i^*) is:

$$v_i^*(v_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 1.82. *The matrix of b with respect to the basis $(v_i)_{1 \leq i \leq n}$ and $(v_i^*)_{1 \leq i \leq n}$ is the symmetric matrix of V associated to $(v_i)_{1 \leq i \leq n}$.*

Proof. From $b(v_i)(v_j) = v_i \cdot v_j$ follows

$$b(v_i) = \sum_{j=1}^n (v_i \cdot v_j) v_j^*.$$

□

As a corollary,

Corollary 1.83. *A quadratic module over F is nondegenerate if and only if the $\text{disc}(Q)$ is nonzero as an element of $\mathbb{K}^\times / \mathbb{K}^{\times 2}$.*

Definition 1.84. Let $U_1, \dots, U_m$ be vector spaces of V . One says that V is the **orthogonal direct sum** of the U_i if they are pairwise orthogonal and V is the direct sum of them. In such case, we write:

$$V = U_1 \hat{\oplus} \dots \hat{\oplus} U_m.$$

Following the remark present in [Ser73, page 28], one has the following.

Remark 1.85. If $x \in V$ has for components x_i in U_i ,

$$Q(x) = Q_1(x_1) + \dots + Q_m(x_m),$$

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 gives $V = \oplus U_i$, with a quadratic form Q , called the direct sum of Q_i , and one has $V = U_1 \hat{\oplus} \dots \hat{\oplus} U_m$.

As an obvious consequence we have the next proposition, which follows from Proposition 2 in [Ser73, page 28].

Proposition 1.86. *Let (V, Q) be nondegenerate. The quadratic module U is nondegenerate if and only if $U^\perp$ is nondegenerate, in which case $V = U \hat{\oplus} U^\perp$. Thus, if V is the orthogonal direct sum of two subspaces, they are nondegenerate and each of them is orthogonal to the other. Moreover,*

$$\text{disc}(Q) = \text{disc}(Q|_U) \times \text{disc}(Q|_{U^\perp}).$$

Proof. If U is a vector subspace then the homomorphism $b_U : V \rightarrow U^*$ defined by $b(x)(y) = x \cdot y$, with $y \in U$, is surjective. In fact, it is obtained by composing $b : V \rightarrow V^*$ defined above, with the canonical surjection $V^* \rightarrow U^*$, and we have supposed that b is bijective. Therefore, we have an exact sequence:

$$0 \rightarrow U^\perp \rightarrow V \rightarrow U^* \rightarrow 0,$$

hence $\dim V = \dim U^* + \dim U^\perp = \dim U + \dim U^\perp$. Therefore, U and $(U^\perp)^\perp$ have the same dimension, and since U is contained in $(U^\perp)^\perp$, we have $U = (U^\perp)^\perp$. The formula $\text{rad}(U) = U \cap U^\perp$ is clear, so if we apply it to $U^\perp$, taking into account that $(U^\perp)^\perp = U$, we get $\text{rad}(U^\perp) = \text{rad}(U)$, and the result follows. The discriminant part is an easy consequence of the above discussion. $\square$

Now, if we assume that (V, Q) is nondegenerate, we define, based on [Shi10, page 116], the **orthogonal group** of Q and the **special orthogonal group** of Q as:

$$\begin{aligned} O(Q) &= O(V) = \{\alpha \in GL_k(V) \mid \alpha^t Q(x) \alpha = Q(x) \text{ for every } x \in V\}, \\ SO(Q) &= SO(V) = \{\alpha \in O(V) \mid \det(\alpha) = 1\}. \end{aligned}$$

Definition 1.87. An element x of a quadratic module (V, Q) is called **isotropic** if $Q(x) = 0$. A subspace U of V is called isotropic if all of its elements are isotropic.

We have evidently,

$$U \text{ isotropic} \Leftrightarrow U \subset U^\perp \Leftrightarrow Q|_U = 0.$$

Definition 1.88. A quadratic module having a basis formed of two isotropic elements x, y such that $x \cdot y \neq 0$ is called a hyperbolic plane.

Remark 1.89. We can always suppose that $x \cdot y = 1$, otherwise we just need to multiply y by $1/(x \cdot y)$. Then the matrix of the quadratic form with respect to x and y is simply $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and its discriminant is -1 , which means that, in particular, it is nondegenerate.

The next proposition is the same as Proposition 3 present in [Ser73, page 29].

Proposition 1.90. *Let $x \neq 0$ be an isotropic element of a nondegenerate quadratic module (V, Q) . Then, there exists a subspace U of V which contains x , and which is a hyperbolic plane.*

Proof. Since V is nondegenerate, there exists $z \in V$ such that $x \cdot z = 1$. Therefore, the element $y = 2z - (z \cdot z)x$ is isotropic and $x \cdot y = 2$. The subspace $U = \mathbb{K}x + \mathbb{K}y$ has the desired property. $\square$

Definition 1.91. A basis $(e_1, \dots, e_n)$ of a quadratic module (V, Q) is called **orthogonal** if its elements are pairwise orthogonal, i.e., if

$$V = \mathbb{K}e_1 \hat{\oplus} \dots \hat{\oplus} \mathbb{K}e_n.$$

This is simply saying that the matrix of Q with respect to this basis is the diagonal matrix

$$\begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_n \end{pmatrix}.$$

If $x = \sum x_i e_i$, then $Q(x) = a_1 x^2 + \dots + a_n x_n^2$.

Following the discussion present in [Lam05, page 8], we have:

Remark 1.92. Let (V, Q) be a quadratic module of rank n and $\text{disc}(Q)$ its discriminant. If $(e_1, \dots, e_n)$ is an orthogonal basis of V , and if we put $a_i = e_i \cdot e_i$, we have

$$\text{disc}(Q) = a_1 \cdots a_n \text{ (in } \mathbb{K}^\times / \mathbb{K}^{\times 2} \text{)}.$$

Theorem 1.93. Every quadratic module (V, Q) has an orthogonal basis.

This is essentially the proof of Theorem 1 in [Ser73, page 29].

Proof. Let (V, Q) be a quadratic module. Since $\text{rad}(V)$ is an orthogonal summand of V , we can assume that V is nondegenerate. Suppose that $Q(x) = 0$ for all $x \in V$. Then for any $x, y \in V$

$$x \cdot y = 0,$$

which implies that $\text{rad}(V) = V$ which is impossible. Now, if we choose a non isotropic vector $x \in V$, then $\mathbb{K}x$ is a nondegenerate subspace, and hence we have a decomposition $V = \mathbb{K}x \hat{\oplus} V'$, where V' is the orthogonal complement of x , so it is nondegenerate. An inductive argument on the dimension of V' completes the proof. □

Let $f(X) = \sum_{i=1}^n a_{ii} X_i^2 + 2 \sum_{i < j} a_{ij} X_i X_j$ be a quadratic form in n variables over k , we put $a_{ij} = a_{ji}$ if $i > j$ so that the matrix $A = (a_{ij})$ is symmetric. The pair $(\mathbb{K}^n, f)$ is a quadratic module associated to f .

Definition 1.94. Two quadratic forms f and f' are called **equivalent** if the corresponding modules are isomorphic. In this case, we write $f \sim f'$.

If A and A' are the matrices of two equivalent forms f and f' , then we are saying that there exists an invertible matrix X such that:

$$A' = X^t A X.$$

Definition 1.95. Let $f(X_1, \dots, X_n)$ and $g(X_1, \dots, X_m)$ be quadratic forms. We denote $f + g$ the quadratic form:

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

in $n + m$ variables. This operation corresponds to the orthogonal sum defined in 1.84.

Similarly we can define $f - g$ for $f + (-g)$.

Definition 1.96. A form $f(X_1, X_2)$ in two variables is called hyperbolic if we have

$$f \sim X_1 X_2 \sim X_1^2 - X_2^2.$$

Definition 1.97. We say that a form $f(X_1, \dots, X_n)$ represents an element a of F if there exists $x \in \mathbb{K}^n$, $x \neq 0$, such that $f(x) = a$.

In particular, f represents 0 if and only if the corresponding quadratic module contains a nonzero isotropic element. The next proposition follows from proposition 3' present in [Ser73, page 33].

Proposition 1.98. *If f represents 0 and is nondegenerate, one has $f \sim f_2 + g$ where f_2 is hyperbolic. Moreover, f represents all elements of $\mathbb{K}$.*

The following proposition determines essentially the same as Corollary 1 present in [Ser73, p. 33], and is simply a translation of Proposition 1.90.

Proposition 1.99. *Let $g = g(X_1, \dots, X_{n-1})$ be a nondegenerate quadratic form and let $a \in \mathbb{K}^\times$. The following properties are equivalent:*

1. g represents a .
2. $g \sim h + aZ^2$, where h is a form in $n - 2$ variables.

Proof. It is clear that $2 \Rightarrow 1$. Conversely, if g represents a , then the quadratic module V contains an x such that $g(x) = a$, meaning $x \cdot x = a$. If H is the orthogonal complement of x , we have $V = H \hat{\oplus} kx$, hence $g \sim g + aZ^2$, where h is the quadratic form corresponding to a basis of H . $\square$

There is a translation of Theorem 1.93 into the classical decomposition of quadratic forms:

Proposition 1.100. *Let f be a quadratic form in n variables. There exist $a_1, \dots, a_n \in \mathbb{K}$ such that $f \sim a_1 X_1^2 + \dots + a_n X_n^2$.*

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 $a_1 \dots a_n$ of f is different from 0 (when f is nondegenerate).

1.3.1 Quadratic forms over finite fields

We can now focus our study in the quadratic forms over $\mathbb{F}_q$, where $q = p^m$ is a power of a prime $p \neq 2$.

Proposition 1.101. *A quadratic form over $\mathbb{F}_q$ of rank ≥ 2 represents all elements of $\mathbb{F}_q^\times$.*

The proof of this proposition is basically the same as the one of Proposition 4 present in [Ser73, page 34], with some slight modifications.

Proof. Given $a, b, c \in \mathbb{F}_q$ nonzero, we must prove that the equation

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

has a solution. Consider the sets,

$$A = \left\{ ax^2 \mid x = 0, 1, \dots, \frac{p-1}{2} \right\}$$

$$B = \left\{ c - by^2 \mid y = 0, 1, \dots, \frac{p-1}{2} \right\}$$

In each of these sets we have precisely $\frac{q+1}{2}$ elements, however there are only q different residue classes thus $A \cap B \neq \emptyset$, from which we get a solution of the equation. □

Recall now that the group $\mathbb{F}_q^\times / \mathbb{F}_q^{\times 2}$ has two elements. Let a denote an element of $\mathbb{F}_q^\times$ which is not a square. The following proposition is present in [Ser73, page 34].

Proposition 1.102. *Every nondegenerate quadratic form of rank n over $\mathbb{F}_q$ is equivalent to*

$$X_1^2 + \dots + X_{n-1}^2 + X_n^2$$

or

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

depending on whether its discriminant is a square or not.

Proof. This is clear when $n = 1$. If $n \geq 2$, Proposition 1.101 shows that the form f represents 1. Thus, by Proposition 1.99 it is equivalent to $X_1^2 + g$ where g is a form in $n - 1$ variables, and we can apply the inductive hypothesis to g . □

Corollary 1.103. *For two degenerate quadratic forms over $\mathbb{F}_q$ to be equivalent it is necessary and sufficient that they have same rank and same discriminant.*

Lemma 1.104. *Every nondegenerate binary quadratic form $F(x, y)$ is equivalent over $\mathbb{F}_p$ to $x^2 - ty^2$ for some $t \in \mathbb{F}_p$.*

Proof. We know that, since p is odd, we can diagonalize the form, so we can assume $F(x, y) = \alpha x^2 + \beta y^2$, for some $\alpha, \beta \in \mathbb{F}_p$. Since it has discriminant $\alpha\beta$, from the last proposition we get that this form is equivalent to the form $x^2 + \alpha\beta y^2$. □

1.4 The projective space

This section provides a general approach to the projective space, particularly the finite projective space. We develop the concepts necessary to introduce the notion of conics and present results that will be helpful in Chapter 2. Our primary references are Chapter 1 of [Rei88] and Chapter 10 of [IR90].

Throughout this chapter, $\mathbb{K}$ is a field. Consider the following equivalence relation between vectors of length 3 with coordinates in $\mathbb{K}$:

$$(X, Y, Z) \sim (X', Y', Z') \Leftrightarrow \exists \lambda \in \mathbb{K}^\times : (X', Y', Z') = \lambda(X, Y, Z).$$

Using this relation we have the following definition,

Definition 1.105. The **projective plane** $\mathbb{P}^2$ is defined as

$$\mathbb{P}^2(\mathbb{K}) = \frac{\mathbb{K}^3 \setminus \{(0, 0, 0)\}}{\sim}.$$

The elements in $\mathbb{P}^2(\mathbb{K})$ corresponding to the equivalence class of (X, Y, Z) are denoted as $[X : Y : Z]$. These elements are called points of $\mathbb{P}^2$ with coordinates in $\mathbb{K}$. We can generalize the definition to all dimensions as follows:

Definition 1.106. The n -dimension projective space $\mathbb{P}^n$ is

$$\mathbb{P}^n(\mathbb{K}) = \frac{\mathbb{K}^{n+1} \setminus \{(0, 0, 0)\}}{\sim},$$

where $(X_0, X_1, \dots, X_n) \sim (X'_0, X'_1, \dots, X'_n) \Leftrightarrow \exists \lambda \in \mathbb{K}^\times : (X'_0, X'_1, \dots, X'_n) = \lambda(X_0, X_1, \dots, X_n)$. The equivalence class of $(X_0, X_1, \dots, X_n)$ is denoted $[X_0 : X_1 : \dots : X_n]$.

The case where $n = 1$ deserves a better look.

Definition 1.107. The **projective line** $\mathbb{P}^1$ is defined as,

$$\mathbb{P}^1(\mathbb{K}) = \frac{\mathbb{K}^2 \setminus \{(0, 0)\}}{\sim},$$

where $(X, Y) \sim (\lambda X, \lambda Y)$ for some $\lambda \in \mathbb{K}^\times$.

Proposition 1.108. $\mathbb{P}^1(\mathbb{F}_p)$ has $p + 1$ points.

Proof. The points in $\mathbb{P}^1(\mathbb{F}_p)$ are of the form $[X : Y]$ with $X, Y \in \mathbb{F}_p$ and at least one is nonzero. We have two disjoint cases. If Y is not zero, then $[X : Y] = \left[\frac{X}{Y} : 1\right]$ and so any $x \in \mathbb{F}_p$ is sent to $(x : 1)$ in $\mathbb{P}^1(\mathbb{F}_p)$, which gives us p points. If Y is zero, then X cannot be zero, and so $[X : 0] = \left[\frac{X}{X} : 0\right] = [1 : 0]$, giving us only one point of this form. We conclude that:

$$\mathbb{P}^1(\mathbb{F}_p) = \{[x : 1] \mid x \in \mathbb{F}_p\} \cup \{[1 : 0]\},$$

and so $\mathbb{P}^1(\mathbb{F}_p)$ has $p + 1$ points. □

From the previous proof, we can see that $\mathbb{P}^1(\mathbb{F}_p)$ is like “ $\mathbb{F}_p$ with one extra point.” We have a similar situation in the case of the projective plane $\mathbb{P}^2(\mathbb{F}_p)$.

Proposition 1.109. $\mathbb{P}^2(\mathbb{F}_p)$ has $p^2 + p + 1$ points.

Proof. The points in $\mathbb{P}^2(\mathbb{F}_p)$ are of the form $[X : Y : Z]$ with $X, Y, Z \in \mathbb{F}_p$, and at least one is nonzero. If Z is not zero, then $[X : Y : Z] = \left[\frac{X}{Z} : \frac{Y}{Z} : 1\right]$. Therefore, we can identify all points (x, y) of $\mathbb{F}_p^2$ as $(x, y) \mapsto [x : y : 1]$, so we have p^2 points. If Z is zero, then we have $[X : Y : 0]$ with at least one of X or Y nonzero, and the number of these points is the same as $\mathbb{P}^1(\mathbb{F}_p)$, since we can map $[X : Y]$ to $[X : Y : 0]$. We have then:

$$\mathbb{P}^2(\mathbb{F}_p) = \{[x : y : 1] \mid x, y \in \mathbb{F}_p\} \cup \{[X : Y : 0] \mid [X : Y] \in \mathbb{P}^1(\mathbb{F}_p)\}, \quad (1.14)$$

and so $\mathbb{P}^2(\mathbb{F}_p)$ has $p^2 + p + 1$ points. $\square$

We call the usual lines in $\mathbb{K}$ **affine lines** and denote them $\mathbb{A}^1(\mathbb{K})$. Similarly, the usual plane is denoted $\mathbb{A}^2(\mathbb{K})$. To better understand the concept of lines in the projective space, recall that the affine lines in the affine space are described by equations of the form $y = mx + b$, where m and b are constants in $\mathbb{K}$. If we replace x and y by $\frac{X}{Z}$ and $\frac{Y}{Z}$, respectively, we find an equation of the form $Y = mX + bZ$, which is a linear equation in our projective space. Thus, we have the following,

Definition 1.110. A **projective line** in $\mathbb{P}^2$ defined over $\mathbb{K}$ is an equation of the form:

$$aX + bY + cZ = 0, \quad (1.15)$$

with constants $a, b, c \in \mathbb{K}$ such that at least one of them is nonzero.

Notice that the set of solutions of a line $L : aX + bY + cZ = 0$ is a well-defined subset of the projective plane $\mathbb{P}^2(\mathbb{K})$. This is because if $[X : Y : Z] \in \mathbb{P}^2(\mathbb{K})$ is such that $aX + bY + cZ = 0$, then given any others X', Y', Z' with $(X', Y', Z') \in [X : Y : Z]$, one has $(X', Y', Z') = \lambda(X, Y, Z)$, so $aX' + bY' + cZ' = \lambda(aX + bY + cZ) = 0$. Which implies that all the elements in the equivalence class satisfy the equation, and the set of solutions is well-defined.

Definition 1.111. Given a projective line $L : aX + bY + cZ = 0$, we denote its set of solutions by $L(\mathbb{K})$.

Definition 1.112. Two equations,

$$L : aX + bY + cZ = 0,$$

$$L' : a'X + b'Y + c'Z = 0,$$

represent the same line if and only if there is a $\lambda \in \mathbb{K}^\times$ such that $a' = \lambda a$, $b' = \lambda b$, $c' = \lambda c$.

It is straightforward to show the following proposition.

Proposition 1.113. Any two distinct lines L and L' defined over $\mathbb{K}$ intersect in exactly one point in $\mathbb{P}^2(\mathbb{K})$.

Proof. We know that lines in the projective space correspond to 2-dimensional linear subspaces of $\mathbb{K}^3$. Since L and L' are distinct, we have that the intersection of the L and L' must have dimension 1. This follows from the fact that it cannot be 2-dimensional, otherwise the L and L' would be the same, and it cannot be 0, since we are looking for $[X : Y : Z]$ such that

$$\begin{cases} aX + bY + cZ = 0 \\ a'X + b'Y + c'Z = 0, \end{cases}$$

and the number of equations is less than the number of variables. So, there must exist a non-trivial solution. Therefore, the intersection is a 1-dimensional subspace, which means that there is a unique equivalence class $[X : Y : Z]$ of nonzero solutions. $\square$

Proposition 1.114. *Through any two distinct points in $\mathbb{P}^2(\mathbb{K})$ passes exactly one projective line.*

Proof. We know that points in the projective space correspond to 1-dimensional linear subspaces of $\mathbb{K}^3$. Let $[X : Y : Z]$ and $[X' : Y' : Z']$ be two distinct points in $\mathbb{P}^2(\mathbb{K})$. If we consider the matrix:

$$M = \begin{pmatrix} X & Y & Z \\ X' & Y' & Z' \end{pmatrix},$$

we are looking for a, b and c in $\mathbb{K}$ such that $M \cdot \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

Since the two points are distinct, the matrix M has rank two, and so its kernel must be one dimensional. Therefore, there exists a nonzero solution (a, b, c) , unique up to scalar multiplication, which means that there is a unique projective line $aX + bY + cZ = 0$. $\square$

Remark 1.115. There is a bijection between the set of all lines in $\mathbb{P}^2$ and $\mathbb{P}^2$ by sending the line $aX + bY + cZ = 0$ to $[a : b : c]$.

Corollary 1.116. *Let $P \in \mathbb{P}^2(\mathbb{K})$ and let L_0 be a line in $\mathbb{P}^2$ defined over $\mathbb{K}$ such that $P \notin L_0$. Then, there is a bijection between all lines L defined over $\mathbb{K}$ passing through P and the set $L_0(\mathbb{K})$.*

Proof. The bijection is given by sending a line L to the intersection of L_0 and L . If L is a line passing through P , then it is distinct from L_0 , therefore it intersects in L_0 in exactly one point $Q \in \mathbb{P}^2(F)$, by Proposition 1.113. Conversely, if Q is a point in the line L_0 , then there is a unique line L passing through P and Q , by Proposition 1.114. $\square$

Given two points $P_0 = [X_0 : Y_0 : Z_0]$ and $P_1 = [X_1 : Y_1 : Z_1]$, if we want to parametrize the line that passes through these points, we consider

$$\ell : [s : t] \mapsto [sX_0 + tX_1 : sY_0 + tY_1 : sZ_0 + tZ_1]$$

as $[s : t]$ varies in $\mathbb{P}^1(F)$. If $[s : t] = [1 : 0]$, we have the point P_0 and when $[s : t] = [0 : 1]$, we have P_1 . If we replace $[s : t]$ by $[\lambda s : \lambda t]$, for some $\lambda \in \mathbb{K}^\times$, we will only multiply the points by λ .

Therefore, the above map is a well-defined map from $\mathbb{P}^1(\mathbb{K})$ to a subset of $\mathbb{P}^2(\mathbb{K})$, and the image is, in fact, the unique projective line that passes through the points P_0 and P_1 . Even though this parametrization is not unique, this is the unique parametrization such that $\ell([1 : 0]) = P_0$ and $\ell([0 : 1]) = P_1$. To recover the equation of the line, we only need to set,

$$\begin{aligned} X &= sX_0 + tX_1 \\ Y &= sX_0 + tX_1 \\ Y &= sX_0 + tX_1, \end{aligned}$$

and eliminate the coordinates s and t . By doing so, we get the equation,

$$(Y_0Z_1 - Y_1Z_0)X + (Z_0X_1 - Z_1X_0)Y + (X_0Y_1 - X_1Y_0)Z = 0.$$

1.4.1 Projective curves: Conics

With all the constructions made, we can extend our study to more general curves other than lines. Our main focus are conics in the projective space, since they are used in Chapter 2. We start with their definition, prove some elementary properties, and prove that there is a bijection between nondegenerate conics and the projective line.

Definition 1.117. A nonzero polynomial $F \in \mathbb{K}[X, Y, Z]$ is **homogeneous** if all monomials appearing have the same constant degree, called the degree of F .

Lemma 1.118. Given an homogeneous polynomial $F \in \mathbb{K}[X, Y, Z]$, the solution set of $F = 0$ is a well-defined subset of $\mathbb{P}^2(\mathbb{K})$.

Proof. Let $\lambda \in \mathbb{K}^\times$. If $a + b + c = d$, then $(\lambda X)^a(\lambda Y)^b(\lambda Z)^c = \lambda^d X^a Y^b Z^c$. We deduce that, for any homoxgeneous F of degree d ,

$$F(\lambda X, \lambda Y, \lambda Z) = \lambda^d F(X, Y, Z).$$

Thus, if (X, Y, Z) is a solution of $F = 0$, so is $(\lambda X, \lambda Y, \lambda Z)$. □

One can wonder how to get a projective equation from an affine one. For instance, if we have the equation:

$$x^2 + y^2 + 1 = 0$$

and we replace x with X/Z and y with Y/Z , we get

$$\frac{X^2}{Z^2} + \frac{Y^2}{Z^2} + 1 = 0$$

$$X^2 + Y^2 + Z^2 = 0,$$

arriving to a homegenous polynomial of degree 2. This processs can be generalized.

Definition 1.119. If $f \in \mathbb{K}[x, y]$ we define the **homogenization** F of f as $F = Z^d f(X/Z, Y/Z)$, where d is the the degree of f .

Definition 1.120. A **conic** in $\mathbb{P}^2$ defined over $\mathbb{K}$ is an equation of the form

$$C : a_0X^2 + a_1XY + a_2XZ + a_3Y^2 + a_4YZ + a_5Z^2 = 0,$$

where $a_0, \dots, a_5$ are constants in $\mathbb{K}$, which are not all equal to zero.

Thus, conics in the projective space are defined by a homogeneous polynomial of degree 2.

Definition 1.121. A conic $F = 0$ is **degenerate** if the quadratic polynomial F is the product of two linear polynomials over some field containing $\mathbb{K}$. Otherwise, the conic is nondegenerate.

From last section we have the following result that is present in [Rei88, page 14], which allows us to classify conics in $\mathbb{P}^2$.

Proposition 1.122. *There are natural bijections,*

$$\left\{ \begin{array}{c} \text{homogeneous} \\ \text{quadratic polynomials} \end{array} \right\} = \left\{ \begin{array}{c} \text{quadratic forms} \\ k^3 \rightarrow k \end{array} \right\} \xleftrightarrow{\text{bij}} \left\{ \begin{array}{c} \text{symmetric bilinear} \\ \text{forms on } k^3 \end{array} \right\},$$

given in formulas by

$$aX^2 + 2bXY + cY^2 + 2dXZ + 2eYZ + fZ^2 \longleftrightarrow \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & f \end{pmatrix}.$$

Recall that a quadratic form is nondegenerate if the corresponding bilinear form is nondegenerate, that is, the determinant of its matrix is nonzero.

Corollary 1.123. *In a suitable system of coordinates, any conic in $\mathbb{P}^2(\mathbb{R})$ is one of the following:*

1. *nondegenerate conic, $C : (X^2 + Y^2 - Z^2 = 0)$;*
2. *empty set, given by $(X^2 + Y^2 + Z^2 = 0)$;*
3. *line pair, given by $(X^2 - Y^2 = 0)$;*
4. *one point $(0, 0, 1)$, given by $(X^2 + Y^2 = 0)$;*
5. *double line, given by $(X^2 = 0)$.*

The proof is basically the same as corollary 1.6 of [Rei88, page 15], with some adaptations.

Proof. Recall that Theorem 1.93 implies that, for a quadratic form Q there exists a basis of V such that $Q(x) = a_1x^2 + \dots + a_nx_n^2$. Now, any real number a_i is either 0, or $\pm$ a square, so we only have to consider Q as in the Theorem 1.93 with $a_i = 0$ or ± 1 . In addition, since we are only interested in the solutions of $Q = 0$, we are allowed to multiply Q by -1 .

□

The subsequent discussion is presented in Section 1.7 of [Rei88, pages 15 and 16].

Let C be a nondegenerate, nonempty conic of $\mathbb{P}^2(\mathbb{R})$. Then, by Corollary 1.123, taking new coordinates $(X + Z, Y, Z - X)$, gives us that C is equivalent to the curve $XZ = Y^2$. This curve is parametrized by:

$$\begin{aligned}\Phi : \mathbb{P}^1(\mathbb{R}) &\longrightarrow C \subset \mathbb{P}^2(\mathbb{R}), \\ [U : V] &\mapsto [U^2 : UV : V^2].\end{aligned}$$

The inverse map $\Psi : C \rightarrow \mathbb{P}^1(\mathbb{R})$ is given by:

$$[X : Y : Z] \mapsto \begin{cases} [X : Y] & \text{if } X \neq 0 \\ [Y : Z] & \text{if } Z \neq 0. \end{cases}$$

Then, Φ and Ψ are inverse isomorphisms. The same thing holds true for any nonempty, nondegenerate conic over a field of characteristic different than 2, since exercise 1.5 of [Rei88] states that a non-empty non degenerate conic $C \subset \mathbb{P}^2(\mathbb{K})$ is projectively equivalent to $XY = Z^2$, which can be seen as a consequence of Proposition 1.98. From the precedent discussion follows that:

Theorem 1.124. *Let C be a nondegenerate conic defined over $\mathbb{K}$. The set of solutions, $C(\mathbb{K})$, of the conic is empty or there is a bijection between $C(\mathbb{K})$ and $\mathbb{P}^1(\mathbb{K})$.*

Corollary 1.125. *The number of points of a nondegenerate conic defined over $\mathbb{F}_p$ is $p + 1$.*

The above corollary is also discussed in [IR90, pages 141 and 142].

Let $F(U, V) \in \mathbb{K}[U, V]$ be a nonzero homogeneous polynomial of degree d .

$$F(U, V) = a_d U^d + a_{d-1} U^{d-1} V + \cdots + a_i U^i V^{d-i} + \cdots + a_0 V^d.$$

F has an associated inhomogeneous polynomial in 1 variable,

$$f(u) = F(u, 1) = a_d u^d + a_{d-1} u^{d-1} + \cdots + a_i u^i + \cdots + a_0.$$

It is not hard to see that for $\alpha \in \mathbb{K}$,

$$\begin{aligned}f(\alpha) = 0 &\Leftrightarrow (u - \alpha) \mid f(u) \\ &\Leftrightarrow (U - \alpha V) \mid F(U, V) \iff F(\alpha, 1) = 0.\end{aligned}$$

so zeros of f correspond to zeros of F on $\mathbb{P}^1$ that are not the point $[1 : 0]$, and for this point one has:

$$F(1, 0) = 0 \Leftrightarrow a_d = 0 \Leftrightarrow \deg f < d.$$

We have the following definition ([Rei88, page 16]).

Definition 1.126. The **multiplicity** of a zero of F on $\mathbb{P}^1$ is:

1. the multiplicity of f at the corresponding $\alpha \in \mathbb{K}$,

2. $d - \deg f$ if $[1 : 0]$ is the zero.

From the previous definition follows that the multiplicity of zero of F at a point $(\alpha, 1)$ is the greatest power of $(U - \alpha V)$ dividing F , and at $[1, 0]$ it is the greatest power of V dividing F .

Proposition 1.127. *Let $F(U, V)$ be a nonzero homogeneous polynomial of degree d . Then F has at most d zeros on $\mathbb{P}^1$. Moreover, if $\mathbb{K}$ is algebraically closed, then F has exactly d zeros on $\mathbb{P}^1$ provided these are counted with multiplicities as defined above.*

The proof can be found in [Rei88, page 17].

Proof. Let m_∞ be the multiplicity of the zero of F at $(1, 0)$; then, by definition, $d - m_\infty$ is the degree of the inhomogeneous polynomial f , and the proposition reduces to the fact that a polynomial in one variable has at most $\deg f$ roots. $\square$

The next theorem is an easy case of the Bézout's theorem, and which is presented in [Rei88, page 17].

Theorem 1.128. *Let $L \subset \mathbb{P}^2(\mathbb{K})$ be a line, and let $D \subset \mathbb{P}^2(\mathbb{K})$ be a curve defined by $D : F_d(X, Y, Z) = 0$, where F is a homogeneous polynomial of degree d . Assuming that $L \not\subset D$ we have:*

$$\#\{L \cap D\} \leq d.$$

If $\mathbb{K}$ is algebraically closed then equality holds.

Proof. A line $L \subset \mathbb{P}^2(\mathbb{K})$ is by definition an equation $L : aX + bY + cZ = 0$. To prove our statement, it is easier if we parameterize the line as,

$$X = \alpha(U, V), \quad Y = \beta(U, V), \quad Z = \gamma(U, V),$$

where α, β, γ are linear forms in U, V . If, for instance, $c \neq 0$, then L can be given as,

$$X = U, \quad Y = V, \quad Z = -\frac{a}{c}U - \frac{b}{c}V.$$

Then the intersection of L with D is given by finding the points $[U : V]$, such that

$$G(U, V) = F_d(\alpha(U, V), \beta(U, V), \gamma(U, V)) = 0.$$

But G is a homogeneous polynomial of degree d , so by Proposition 1.127, we have what we desired. $\square$

Chapter 2

The Metacommutation Problem

Even though the Hurwitz integers are not commutative, they have a very intriguing property, called metacommutation, that derives from Theorem 1.20. The metacommutation problem was first stated in [CS03] and was later studied in detail in [CK15] and [FGS15], all of which are the foundations of this chapter. We first introduce the Metacommutation problem and then we study in detail a permutation, which we call the metacommutation map. In particular, we are interested in its fixed points and sign of permutation. We also provide some insights into the cycle structure of this permutation that work as the base of Chapter 3.

2.1 Metacommutation map

A direct consequence of Theorem 1.20, is the fact that, given a Hurwitz integer, say h , if we want to investigate all of its factorizations, we need to allow possible changes in the factorization of its norm. For example, if $N(h) = 60 = 2^2 \times 3 \times 5$, then we have 12 factorizations of h , up to unit-migration.

We focus on the particular case where our Hurwitz integer is a product of two Hurwitz primes. For instance, consider the case where P and Q are primes such that $N(P) = p$ and $N(Q) = q$ are different rational primes. It follows immediately from Theorem 1.20 that we can find primes Q' and P' of norms q and p , satisfying:

$$PQ = Q'P', \tag{2.1}$$

where $Q'P'$ is modeled on qp and is unique up to unit-migration. This process of switching adjacent primes is called metacommutation and was first introduced by Conway and Smith in Chapter 5 of [CS03]. It is clear that we have an equivalence relation, where the equivalence class of P , which is the set of left associates of P , is denoted by $[P]$, and the set consisting of these classes is denoted Π_p , as in 1.36. With this in mind we are now in conditions to define the metacommutation map.

Definition 2.1. Given a quaternion Q of norm q prime and a rational prime p , the map

$$\begin{aligned} \tau_{Q,p} : \Pi_p &\rightarrow \Pi_p \\ [P] &\mapsto [P'], \end{aligned}$$

where Π_p is the set defined in 1.36 and P' is obtain from P by the previous relation $PQ = Q'P'$, is the **metacommutation map** by Q of primes of norm p .

One should notice that P' is defined up to left multiplication by an unit and that replacing P by a left associate has no effect on P' as we can see by the equation $(uP)Q = (uQ')P'$, therefore $\tau_{Q,p}$ is well defined.

Proposition 2.2. *Let Q be a Hurwitz integer and p a rational prime. The metacommutation map $\tau_{Q,p}$, is a permutation of the primes lying above p .*

Proof. Since we have a map defined on a finite set, we just need to prove that $\tau_{Q,p}$ is injective.

For instance, consider that exist $P_1, P_2 \in \mathcal{H}$, such that $\tau_Q([P_1]) = \tau_Q([P_2]) = [P]$. Then, there exist Q' and Q'' such that $P_1Q = Q'P$ and $P_2Q = Q''P$. From this we know that

$$\bar{Q}'P_1Q = N(Q)P = \bar{Q}''P_2Q.$$

Then, $\bar{Q}'P_1 = P\bar{Q} = \bar{Q}''P_2$, so by Theorem 1.20, P_1 and P_2 are left associates. Therefore, $[P_1] = [P_2]$, and $\tau_{Q,p}$ is injective. □

Remark 2.3. If τ_Q sends $[P]$ to $[P']$, then $\tau_{\bar{Q}}$, send $[P']$ to $[P]$. Moreover, the cycle structure of the permutation $\tau_{Q,p}$ is the same of the permutation $\tau_{\bar{Q},p}$. This is due to the fact that since $\tau_{Q,p}$ sends $[P]$ to $[P']$, we have that, up to unit-migrations, $PQ = Q'P'$, now

$$\bar{Q}'PQ\bar{Q} = \bar{Q}'Q'P'\bar{Q},$$

thus $\bar{Q}'P = P'\bar{Q}$, and $\tau_{\bar{Q},p}$ sends P' to P .

One can wonder if p and q alone determine the cycle structure. The following examples show that this is not the case.

Example 2.4. Consider $p = 5$, $q = 7$ and let $Q = 1 + 2i + j + k$. Then the permutation has two fixed points and a cycle of length 4. However, if $Q = 2 + i + j + k$, then the permutation is a cycle of length 6.

In fact, the previous example shows that, not only the norms do not determine the cycle structure, but we also can have permutations with and without fixed points. With this idea in mind, we take a closer look at the next example.

Example 2.5 (From Cohn and Kumar). If $p = 13$ and $q = 11$, the number of different primes Q such $N(Q) = 12$ is 288 since there are 12 classes with 24 elements each. We have:

1. For 24 primes Q , the permutation consists in 7 cycles of length 2.
2. For 96 primes Q , the permutation has 2 fixed points and one cycle of length 12.
3. For 72 primes Q , the permutation is a cycle of length 14.
4. For 96 primes Q , the permutation has 2 fixed points and three cycles of length 4.

From this example, several questions naturally arise, because we would like to know when do we have fixed points and how many can we have, since it appears that we can only at most 2 fixed points. It seems that, in the previous scenario, the cycles which are not fixed points have all the same length. In order to answer why does this always happen, Cohn and Kumar proved in [CK15], the following theorem.

Theorem 2.6 (Cohn and Kumar). *Let p and q be distinct rational primes, let Q be a Hurwitz prime of norm q . Then, the sign of the metacommutation map, $\tau_{Q,p}$, is the quadratic character $\left(\frac{q}{p}\right)$ of q modulo p .*

If $p = 2$ or if Q is congruent to a rational integer modulo p , then the map is the identity permutation, otherwise it is $1 + \left(\frac{\text{Tr}(Q)^2 - 4q}{p}\right)$ fixed points.

When $p = 2$, there is only one Hurwitz prime above p as we have already seen in Corollary 1.35. Therefore, the last theorem is trivial in this case, so from now on we assume that p is odd. The main goal of this chapter is to prove Theorem 2.6. In order to do it one must view the metacommutation problem in another way. Thus, and so that everything becomes clear, we will need to introduce new notions before moving to its proof.

2.2 A conic associated to the primes above p

Let P be a Hurwitz prime of odd norm p and consider $[\mathcal{H}]_p = \mathcal{H}/\mathcal{H}p$. We denote $[P]_p$ as the reduction of P modulo p . Then, we can define $[\mathcal{H}P]_p$ as the reduction of the left ideal modulo p , i.e., $[\mathcal{H}P]_p = \{h[P]_p \mid h \in [\mathcal{H}]_p\}$.

The first thing we notice is the upcoming proposition, which is present in [FGS15].

Proposition 2.7. *$[\mathcal{H}]_p$ is isomorphic to $M_2(\mathbb{F}_p)$.*

The proof is similiar to the one of [FGS15].

Proof. We construct the explicit isomorphism $\varphi : [\mathcal{H}]_p \rightarrow M_2(\mathbb{F}_p)$. If $\gamma \in [\mathcal{H}]_p$, and

$$\gamma = \gamma_1 + \gamma_2 i + \gamma_3 j + \gamma_4 k,$$

then

$$\varphi(\gamma) = \begin{pmatrix} \gamma_1 + \gamma_2 a + \gamma_4 b & \gamma_3 + \gamma_4 a - \gamma_2 b \\ -\gamma_3 + \gamma_4 a - \gamma_2 b & \gamma_1 - \gamma_2 a - \gamma_4 b \end{pmatrix},$$

where $a^2 + b^2 \equiv -1 \pmod{p}$. First, we prove that such a and b always exist. For that recall that modulo p there are only p distinct residue classes and consider the sets:

$$A = \left\{ 1 + a^2 \mid a = 0, 1, \dots, \frac{p-1}{2} \right\},$$

$$B = \left\{ -b^2 \mid a = 0, 1, \dots, \frac{p-1}{2} \right\}.$$

In each of these sets we have precisely $\frac{p+1}{2}$ different elements. Therefore, in total we have $p+1$ different residue classes. Since the numbers of different classes is only p , there are two numbers

from different classes which are equal modulo p . Meaning that there exist $a, b \in \mathbb{F}_p$ such that $1 + a^2 \equiv -b^2 \pmod{p}$, or equivalently that $a^2 + b^2 \equiv -1 \pmod{p}$.

It is a straightforward computation to see that φ is a homomorphism. To see that φ is injective, let $\varphi(\gamma) = 0$, then

$$\begin{cases} \gamma_1 + \gamma_2 a + \gamma_4 b = 0 \\ \gamma_3 + \gamma_4 a - \gamma_2 b = 0 \\ -\gamma_3 + \gamma_4 a - \gamma_2 b = 0 \\ \gamma_1 - \gamma_2 a - \gamma_4 b = 0 \end{cases}$$

If we sum the first and last equations, we get that $\gamma_1 = 0$, and then the second minus the third gives us that $\gamma_3 = 0$. With this, we get that $\gamma_2 a + \gamma_4 b = 0$ and $\gamma_4 a - \gamma_2 b = 0$, and so

$$\begin{aligned} a(\gamma_2 a + \gamma_4 b) - b(\gamma_4 a - \gamma_2 b) &= 0 \Leftrightarrow \\ \gamma_2(a^2 + b^2) &= 0. \end{aligned}$$

Therefore, $\gamma_2 = 0$ and $\gamma_4 = 0$. Thus, since φ is a injective ring homomorphism defined on a finite set to a finite set of the same cardinality, it is a isomorphism. $\square$

Notice that if P and P' are left associates, then $[\mathcal{H}P]_p = [\mathcal{H}P']_p$. Again, we are motivated, to consider uniqueness of the primes of norm p up to left multiplication by units. Next, consider the following proposition that is present in [FGS15].

Proposition 2.8. *Let p be a fixed rational prime. Then $\dim([\mathcal{H}P]_p) = 2$.*

Proof. We can see that $[\mathcal{H}P]_p$ is not the zero ideal since it contains $[P]_p$. Also, $[\mathcal{H}P]_p$ is not the entire algebra since it is annihilated by right multiplication by $[\bar{P}]_p$. We know that conjugation is an automorphism of $[\mathcal{H}]_p$, thus $[\mathcal{H}P]_p$ has the same dimension as $[\mathcal{H}\bar{P}]_p$, therefore it can only have dimension 2. $\square$

Remark 2.9. There exists a one to one correspondence between prime ideals in $\mathcal{H}$ and two dimensional left ideals of $[\mathcal{H}]_p$.

Proof. Consider the natural homomorphism map $\pi : \mathcal{H} \rightarrow [\mathcal{H}]_p$ defined by $\pi(h) = h + \mathcal{H}p$. It is a well-known result that there exists a one to one correspondence between ideals of $\mathcal{H}$ that contain $\mathcal{H}p$ and ideals of $[\mathcal{H}]_p$. The ideals that contain $\mathcal{H}p$ are generated by divisors of p , i.e, generated by $1, p$ or primes of norm p . However, only the ideals generated by the latter correspond to proper ideals in $[\mathcal{H}]_p$. $\square$

Therefore, studying the primes of norm p is equivalent to studying proper ideals in $[\mathcal{H}]_p$.

This lets us count the number of Hurwitz primes of norm p through a bijective correspondence with points on the conic:

$$C_p = \left\{ [x : y : z] \in \mathbb{P}^2(\mathbb{F}_p) \mid x^2 + y^2 + z^2 = 0 \right\}.$$

Lemma 2.10. *There is a unique element $t_P = bi + cj + dk$ of trace zero in $[\mathcal{H}P]_p$, up to scaling (multiplication by $\lambda \neq 0$).*

We stick to the proof present in [CK15].

Proof. The trace on the ideal $[\mathcal{H}P]_p$ is a linear function on a two-dimensional space. Thus, it has a non-trivial kernel of dimension at least one. However, the kernel cannot be $[\mathcal{H}P]_p$ itself. In fact, if $x = bi + cj + dk$ is any nonzero element of the kernel, then one of b, c and d is nonzero and so one of ix, jx and kx (which are in $[\mathcal{H}P]_p$ since it is a left ideal) will have nonzero trace. So, the kernel has exactly dimension one and, up to scaling, there is a unique nonzero element,

$$t_P = bi + cj + dk,$$

with trace 0. □

Note that if for $t \in [\mathcal{H}P]_p$ then $N(t)$ must be zero, modulo p , since $t = [hP]_p$ for some $h \in \mathcal{H}$ and $N(hP) = N(h)N(P) = pN(h)$ which is 0 modulo p . In particular, we have that $N(t_P) = 0$ and so,

$$b^2 + c^2 + d^2 = 0.$$

Meaning that for t_P there's a corresponding point $c_P = (b, c, d) \in C_p$.

Proposition 2.11. *There is a bijective correspondence between points on the conic C_p and Hurwitz primes P of norm p .*

The proof we give follows the argument in [CK15].

Proof. As we have seen, primes lying over p correspond to proper ideals of $[\mathcal{H}]_p$, so we only need to deal with those. Given a point $c_P = (b, c, d) \in C_p$, consider the ideal $[\mathcal{H}]_p t_P$. This ideal is nonzero, but it is not the full ring, because if $x \in [\mathcal{H}]_p t_P$, then $xt_P = 0$. Thus, $\dim([\mathcal{H}]_p t_P) = 2$ and $[\mathcal{H}]_p(t_P) = [\mathcal{H}P]_p$. This describes the inverse map and establishes the bijection. □

Remark 2.12. With this bijection in mind and Corollary 1.125, we can recover the count of the number of primes above the odd rational prime p , which is $p + 1$, up to left multiplication by units.

2.3 Metacommutation revisited

We are in conditions to translate the metacommutation problem in terms of the constructions we made in the previous section.

Proposition 2.13. *For $P \in \mathcal{H}$ with norm p , let Q be a Hurwitz prime with norm q and P' and Q' obtained as in 2.1. Then, $[Q]_p^{-1} t_P [Q]_p$ and $t_{P'}$ are equal modulo scaling.*

The proof is essentially the one present in [CK15].

Proof. Because $PQ = Q'P'$, we see that $[PQ]_p$ is contained in $[\mathcal{H}P']_p$, which is a left ideal. Therefore, any left multiple of $[PQ]_p$ is also in $[\mathcal{H}P']_p$, so $[\mathcal{H}P]_p Q \subseteq [\mathcal{H}P']_p$. In fact, since Q' is invertible, $Q'^{-1}PQ = P'$, so $[P']_p$ is contained in $[\mathcal{H}PQ]_p$. Therefore we have that $[\mathcal{H}P']_p = [\mathcal{H}PQ]_p$. Since $[Q]_p$ is invertible, and we are dealing with left ideals,

$$[Q]_p^{-1}[\mathcal{H}P]_p[Q]_p = [\mathcal{H}PQ]_p = [\mathcal{H}P']_p.$$

In particular, since $t_P \in [\mathcal{H}P]_p$, we must have $[Q]_p^{-1}t_P[Q]_p \in [\mathcal{H}P']_p$. However, $[Q]_p^{-1}t_P[Q]_p$ has trace zero and is nonzero, therefore, up to scaling it must be equal to t'_P . □

The Proposition 2.13 is important because it gives a simpler way of thinking about the metacommutation action: as a group action by conjugation of the quaternions with nonzero norm in $[\mathcal{H}]_p$ on the points of C_p . For instance, suppose that $t_P = xi + yj + zk$ and $[Q]_p = a + bi + cj + dk$ with the norm $q = N(Q) = a^2 + b^2 + c^2 + d^2$. Then, it is straightforward to see that $[Q]_p^{-1}t_P[Q]_p = x'i + y'j + z'k \in [\mathcal{H}P]_p$ with $(x', y', z') = \phi_{Q,p}(x, y, z)$ where,

$$\phi_{Q,p} = \frac{1}{q} \begin{pmatrix} a^2 + b^2 - c^2 - d^2 & 2ad + 2bc & -2ac + 2bd \\ -2ad + 2bc & a^2 - b^2 + c^2 - d^2 & 2ab + 2cd \\ 2ac + 2bd & -2ab + 2cd & a^2 - b^2 - c^2 + d^2 \end{pmatrix}.$$

Remark 2.14. Notice that $\phi_{Q,p}$ lies in $SO_3(\mathbb{F}_p)$, which can be easily proved by direct computation. However, one can try to grasp this idea by recalling that, for a quaternion x , $N(x) = x \cdot x = x\bar{x}$. We can think of $N(x)$ as a quadratic form $x\bar{x}$. Hence, $\phi_{Q,p} \in O_3(\mathbb{F}_p)$ because conjugation preserves this quadratic form on quaternions x , since $N(Q^{-1}xQ) = N(x)$. One also has that $\det(\phi_{Q,p}) = 1$ because left or right multiplication by a quaternion Q has determinant $N(Q)^2$ on $[\mathcal{H}]_p$, and so conjugation has determinant 1 as a linear transformation on $[\mathcal{H}]_p$ and consequently, also on the purely imaginary subspace, since the identity element of $[\mathcal{H}]_p$ is fixed.

Remark 2.15. If the vector (b, c, d) is not the zero vector, then it is an eigenvector of $\phi_{Q,p}$ with eigenvalue 1.

Proof. It is easy to see that $bi + cj + dk$ commutes with $[Q]_p$, since their vector parts are colinear (which follows from Remark 1.5). □

Eigenvectors of $\phi_{Q,p}$ that lie on the cone:

$$K_p = \left\{ (x, y, z) \in \mathbb{F}_p^3 \mid x^2 + y^2 + z^2 = 0 \right\},$$

correspond to fixed points of the metacommutation map, since one would have $[Q]_p^{-1}t_P[Q]_p = \lambda t_P$ and from Proposition 2.13, $[Q]_p^{-1}t_P[Q]_p = t'_P$, thus $t'_P = \lambda t_P$, which means that they are the same up to scaling and belong to the same class in C_p . Also from Proposition 2.11, there's a bijection between points on the conic C_p and the primes P of norm p , therefore $P = P'$ when $t'_P = t_P$, up to scaling.

Remark 2.16. The eigenvector (b, c, d) lies on the cone K_p iff $q = a^2$.

Lemma 2.17. *The characteristic polynomial of $\phi_{Q,p}$ is*

$$\chi_{Q,p}(x) = (x-1) \left(x^2 + 2 \left(1 - \frac{2a^2}{q} \right) x + 1 \right)$$

Proof. Since $\phi_{Q,p}$ is a 3×3 matrix we can express its characteristic polynomial as

$$x^3 - \text{Tr}(\phi_{Q,p})x^2 + bx - \det(\phi_{Q,p}), \quad b \in \mathbb{F}_p.$$

We already observed that 1 is always an eigenvalue and that $\det(\phi_{Q,p}) = 1$. Thus,

$$1^3 - \text{Tr}(\phi_{Q,p}) + b - 1 = 0 \Leftrightarrow b = \text{Tr}(\phi_{Q,p}). \quad (2.2)$$

Therefore, to determine its characteristic polynomial, all we need to show is that,

$$\text{Tr}(\phi_{Q,p}) = \frac{4a^2}{q} - 1,$$

but now we see, explicitly that :

$$\text{Tr}(\phi_{Q,p}) = \frac{3a^2 - (b^2 + c^2 + d^2)}{q} = \frac{4a^2}{q} - 1,$$

as desired. So the characteristic polynomial is

$$x^3 - \left(\frac{4a^2}{q} - 1 \right) x^2 + \left(\frac{4a^2}{q} - 1 \right) x - 1,$$

which is equivalent to:

$$(x-1) \left(x^2 + 2 \left(1 - \frac{2a^2}{q} \right) x + 1 \right).$$

□

Notice that the eigenvalue 1 has multiplicity greater than 1 if and only if $q = a^2$, and -1 is an eigenvalue if and only if $a = 0$.

2.4 Fixed points

We can now build upon the work we presented in the last section. Here, we find the fixed points of the permutation $\phi_{Q,p}$ considered as a projective transformation. In particular, we want to find the fixed points that lie on the conic C_p , since those will correspond to the fixed points of the metacommutation map. This is to say that, as we have already seen, we are interested in eigenvectors of $\phi_{Q,p}$ that lie on the cone K_p . With this, we can prove the second part of Theorem 2.6, which we recall.

Theorem 2.18 (Cohn and Kumar). *Let Q be a prime of norm q , with $[Q]_p = a + bi + cj + dk \in \mathcal{H}$. If $b = c = d = 0$, then $\tau_{Q,p}$ is the identity permutation. Otherwise, $\tau_{Q,p}$ has $1 + \left(\frac{a^2 - q}{p} \right)$ fixed points.*

The proof is the same as [CK15], but with some tweaks and more detail.

Proof. We have several cases which we need to analyse.

Case 1. $b = c = d = 0$.

In this case, one can easily see that $\phi_{Q,p}$ is the identity.

Case 2. $q \equiv a^2 \pmod{p}$ but $(b, c, d) \neq (0, 0, 0)$.

The characteristic polynomial is $(x - 1)^3$, i.e., the eigenvalue 1 occurs with multiplicity 3. We already know that (b, c, d) is an eigenvector with eigenvalue 1. Also, this vector is on the cone K_p , since

$$a^2 = q = a^2 + b^2 + c^2 + d^2.$$

We see that, up to scaling, $\phi_{Q,p}$ has no other vectors. Because the eigenvalue must be 1, given another eigenvector, x , we have that it must commute with $[Q]_p$, since $[Q]_p^{-1}x[Q]_p = x$ implies that $x[Q]_p = [Q]_p x$. So, since x is purely imaginary, it must be colinear, in $\mathbb{F}_p$, with the vector part of Q which is precisely (b, c, d) . Therefore, up to scaling, this vector is unique. Thus, we see that $\phi_{Q,p}$ is the identity.

Case 3. $a = 0$.

Then, we have $q = a^2 + b^2 + c^2 + d^2 = b^2 + c^2 + d^2 \neq 0$, and therefore the eigenvector (b, c, d) is not on the cone K_p . The characteristic polynomial of $\phi_{Q,p}$ is

$$\chi_{Q,p}(x) = (x - 1)(x^2 + 2x + 1) = (x - 1)(x + 1)^2,$$

and so the eigenvalue -1 occurs with multiplicity 2. We prove that $\phi_{Q,p}$ is semisimple (for more detail see Appendix A), for that we see that the geometric multiplicity of -1 is also 2. Once again, from the fact that -1 is an eigenvalue, we get that $[Q]_p x = -x[Q]_p$ and, since we know that $\text{Tr}(x) = \text{Tr}([Q]_p) = 0$ we have,

$$\begin{aligned} \text{Tr}(x[Q]_p) = 0 &\Leftrightarrow x[Q]_p + [\bar{Q}]_p \bar{x} = 0 \\ &\Leftrightarrow x[Q]_p + [Q]_p x = 0. \end{aligned}$$

Therefore, $[Q]_p x = -x[Q]_p$ is equivalent to $\text{Tr}(x[Q]_p) = 0$, which is the kernel of $x \rightarrow \text{Tr}(x[Q]_p)$. Since this is a linear operator in the three-dimensional space, its kernel must be at least two dimensional, thus the (-1) -eigenspace is two-dimensional. The last thing we need to see is whether these eigenvectors are in the cone K_p .

If an element $X = (x, y, z)$ is in the (-1) -eigenspace then $[Q]_p X = -X[Q]_p$ is equivalent to

$$-bx - cy - dz = bx + cy + dz \Leftrightarrow bx + cy + dz = 0.$$

For X to be in K_p it must also satisfy,

$$x^2 + y^2 + z^2 = 0.$$

In other words, the points that are in the (-1) -eigenspace and in the cone K_p are given by the solutions of the system

$$\begin{cases} bx + cy + dz = 0 \\ x^2 + y^2 + z^2 = 0 \end{cases}$$

In the projective plane, this is the intersection of a line and a conic, so there are two solutions over the algebraic closure $\bar{\mathbb{F}}_p$, if we count with multiplicity.

From the Lemma 1.128, we know that in $\mathbb{F}_p$, this intersection contains at most 2 points, since C_p is nondegenerate. Also, since $b^2 + c^2 + d^2 \neq 0$, at least one of b^2, c^2, d^2 is nonzero, assuming it is d^2 , we can parametrize the line:

$$L : bx + cy + dz = 0,$$

using the parametrization:

$$\ell(s, t) = (ds, dt, -bs - ct),$$

and plug it in the equation of C_p , we get,

$$\begin{aligned} (ds)^2 + (dt)^2 + (-bs - ct)^2 &= 0, \\ (d^2 + b^2)s^2 + 2bcst + (d^2 + c^2)t^2 &= 0, \end{aligned}$$

which has discriminant:

$$-4d^2(b^2 + c^2 + d^2).$$

We cannot have one solution, since that would imply $b^2 + c^2 + d^2 = 0$, which is impossible. The solutions are defined over $\mathbb{F}_p$ if and only if $-q = -(b^2 + c^2 + d^2)$ is a square in $\mathbb{F}_p$. Thus, there are two distinct points of intersection when $\left(\frac{-q}{1}\right) = 1$ and none when $\left(\frac{-q}{p}\right) = -1$.

Case 4. $a \neq 0$ and $q \neq a^2$.

Then, we have $b^2 + c^2 + d^2 \neq 0$, and so (b, c, d) is not on the cone K_p . In this case, the characteristic polynomial of $\phi_{Q,p}$ is:

$$\chi_{Q,p}(x) = (x - 1) \left(x^2 + 2 \left(1 - \frac{2a^2}{q} \right) x + 1 \right)$$

The quadratic part of the characteristic polynomial has two distinct roots in $\bar{\mathbb{F}}_p$, both not equal to ± 1 . Computing the discriminant of this polynomial, we get $-16a^2(q - a^2)/q^2$, and so there are two eigenvalues in $\mathbb{F}_p$ if $\left(\frac{a^2 - q}{p}\right) = 1$ and none if $\left(\frac{a^2 - q}{p}\right) = -1$. Note that the corresponding eigenvectors are distinct from each other and from (b, c, d) , since they belong to correspond eigenvalues not equal to ± 1 .

Finally, we only have to prove that these eigenvectors belong to the cone, K_p . In fact, if v is one of these eigenvectors, v corresponds to an eigenvalue $\lambda \neq \pm 1$, and so, using the usual inner product defined by the quadratic form $Q(v) = v \cdot v = v\bar{v}$ (where in the last equality we see v as a pure quaternion), we have

$$\lambda^2(v \cdot v) = \lambda v \cdot \lambda v = \phi_{Q,p}(v) \cdot \phi_{Q,p}(v).$$

But, since $\phi_{Q,p}$ is an orthogonal transformation, we have

$$\phi_{Q,p}(v) \cdot \phi_{Q,p}(v) = v \cdot v,$$

and so $\lambda^2(v \cdot v) = v \cdot v$ implies that $v \cdot v = 0$, i.e., v belongs to the cone K_p .

Then, in every case, we proved that $\tau_{Q,p}$ has $1 + \left(\frac{a^2-q}{p}\right)$ fixed points. □

Remark 2.19. Notice that we can only have one fixed point if and only if $a^2 - q = 0$, modulo p . We will see that in this case, the rest of the permutation is a p -cycle.

2.5 Cycle structure and sign of permutation

In this section, our objective is to analyze the cycle structure of the permutation $\tau_{Q,p}$. In particular, we are interested in calculating its sign. In order to prove that the sign is $\left(\frac{p}{q}\right)$, we use results about the special orthogonal group of quadratic forms and conics over finite fields.

Let p be an odd prime and F a nondegenerate quadratic form over $\mathbb{F}_p$. We gather some general results about $SO(F)$ and its action on affine plane conics given by $F(x, y) = u$.

Notice that we know from Lemma 1.104 that every nondegenerate quadratic form $F(x, y)$ is equivalent over $\mathbb{F}_p$ to the diagonal form $g_t(x, y) = x^2 - ty^2$, for some $t \in \mathbb{F}_p \setminus \{0\}$, so from now on we will only work with this form.

Lemma 2.20. *Let $u \in \mathbb{F}_p \setminus \{0\}$. The number of points in the affine conic $x^2 - ty^2 = u$ is $p - \left(\frac{t}{p}\right)$.*

Proof. From Corollary 1.125, we know that the nondegenerate projective conic is isomorphic to $\mathbb{P}^1(\mathbb{F}_p)$, so it has $p + 1$ points. To get back to the affine conic we need to remove the line at infinity and its points. The points that belong to this line satisfy the equation $x^2 - ty^2 = 0$, which has either 0 or 2 solutions, according to the quadratic character of t modulo p . □

Proposition 2.21. *The group $SO(g_t)$ is cyclic of order $p - \left(\frac{t}{p}\right)$. Every element of $SO(g_t)$ is semisimple.*

We follow essentially [CK15] adding more detail when needed.

Proof. Let A be the matrix associated with g_t , meaning it is the matrix

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -t \end{pmatrix}$$

The group $O(g_t)$ is the group of 2×2 invertible matrices that preserve the form. Meaning that, if $X \in O(g_t)$, $X^t A X = A$. Let X be the matrix,

$$X = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$$

Then $X A X^t = A$ implies that $\alpha^2 - t\beta^2 = 1$, $\gamma^2 - t\delta^2 = -t$ and $\alpha\gamma - \beta\delta t = 0 \Leftrightarrow \gamma = \frac{\beta\delta t}{\alpha}$. Also,

$$(\alpha, \beta) \cdot (\gamma, \delta) = (\alpha, \beta) A (\gamma, \delta)^t = \alpha\delta - \beta t = 0$$

So the columns of X are orthogonal with respect to g_t and $(\gamma, \delta) = \pm(\beta t, \alpha)$.

For the matrix to be in $SO(g_t)$, we must have $(\gamma, \delta) = (\beta t, \alpha)$. Thus, the elements of $SO(g_t)$ are matrices of the form

$$M_{\alpha, \beta} = \begin{pmatrix} \alpha & \beta t \\ \beta & \alpha \end{pmatrix}$$

with $\alpha^2 - t\beta^2 = 1$, and by the previous lemma, there are $p - \left(\frac{t}{p}\right)$ such points, so the size of the group is exactly what we wanted. It to see that this group is cyclic and that every element is semisimple. Notice that multiplication of matrices in $SO(g_t)$ follows the group law

$$M_{\alpha, \beta} M_{\gamma, \delta} = M_{\alpha\gamma + \beta\delta t, \alpha\delta + \beta\gamma}.$$

If $t = r^2$ is a square, then $SO(g_t)$ has $p - 1$ elements and we have

$$\alpha^2 - \beta^2 t = \alpha^2 - \beta^2 r^2 = (\alpha - \beta r)(\alpha + \beta r).$$

We see that the map

$$\begin{aligned} \eta : SO(g_t) &\rightarrow \mathbb{F}_p^\times \\ M_{\alpha, \beta} &\mapsto \alpha + \beta r \end{aligned}$$

is an isomorphism of groups. Since both groups have $p - 1$ elements, we only need to see that η is injective. Thus, if

$$\eta(M_{\alpha, \beta}) = 1 \Leftrightarrow \alpha + \beta r = 1,$$

then,

$$1 = \alpha^2 - \beta^2 t = (\alpha - \beta r)(\alpha + \beta r) = (\alpha - \beta r).$$

Thus, we get that $(\alpha - \beta r) = 1$ which, if we sum both equations, gets us $2\alpha = 2$, so $\alpha = 1$ and $\beta = 0$, and therefore $M_{\alpha, \beta}$ is the identity. Since $\mathbb{F}_p^\times$ is cyclic of order $p - 1$ so is $SO(g_t)$. If t is not a square, consider the map:

$$\begin{aligned} \eta : SO(g_t) &\rightarrow \mathbb{F}_{p^2}^\times \\ M_{\alpha, \beta} &\mapsto \alpha + \beta\sqrt{t}. \end{aligned}$$

Since $(\alpha + \beta\sqrt{t})(\alpha - \beta\sqrt{t}) = 1$, we have that

$$\begin{aligned} N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\alpha + \beta\sqrt{t}) &= (\alpha + \beta\sqrt{t})(\alpha + \beta\sqrt{t})^p \\ &= (\alpha + \beta\sqrt{t})(\alpha^p + \beta^p(\sqrt{t})^p) \\ &= (\alpha + \beta\sqrt{t})(\alpha - \beta\sqrt{t}) = 1 \end{aligned}$$

Therefore η gives an isomorphism of $SO(g_t)$ with the subgroup N of elements of $\mathbb{F}_{p^2}^\times$ of norm 1. These are the solutions of $N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(z) = z \times z^p = z^{p+1} = 1$ in $\mathbb{F}_{p^2}^\times$, so there are $p + 1$ solutions. Since N is a finite subgroup of a multiplicative group of a field, it is also cyclic.

In either case, we mapped $M_{\alpha, \beta}$ to one of its eigenvalues. In fact, in the first case r is a square root of t , so both maps are essentially the same. Finally, we still need to see that every element of $SO(g_t)$ is semisimple. The characteristic polynomial of $M_{\alpha, \beta}$ is

$$x^2 - 2\alpha x + 1,$$

which has discriminant $4(\alpha^2 - 1)$. If $\alpha \neq \pm 1$, then the eigenvalues in $\mathbb{F}_p^2$ are distinct, so there are two distinct eigenvalues in $\bar{\mathbb{F}}_p$, hence $M_{\alpha,\beta}$ is semisimple (for more detail see A). If $\alpha = \pm 1$, then $\alpha^2 - t\beta^2 = 1$ implies that $\beta = 0$ and so $M_{\alpha,\beta}$ is either the identity or its negation, so it is semisimple. $\square$

Proposition 2.22. *Let $\psi \in SO(g_t)$ have polynomial $x^2 + (2 - v)x + 1 = (x + 1)^2 - vx$, with $v \neq 0$. Then v is a square in $\mathbb{F}_p$ if and only if*

$$\frac{|SO(g_t)|}{\text{ord}(\psi)}$$

is even.

The following proof is the same as the one in [CK15].

Proof. Since ψ is semisimple, its order is equal to the order of its two eigenvalues, which are reciprocals of each other. Thus, for an eigenvalue λ , we have that

$$\frac{|SO(g_t)|}{\text{ord}(\lambda)}$$

is even iff $\lambda = \delta^2$ where δ is an element in the correspondig cyclic group $F_p^\times$ or N with the notation from the proof of Proposition 2.21.

Again, like in the proof of Proposition 2.21, we first suppose $t = r^2$ is a square, so $SO(g_t) \simeq F_p^\times$. Because the characteristic polynomial is $(x + 1)^2 - vx$, we have $(\lambda + 1)^2 - v\lambda = 0$ and so

$$v = \frac{(\lambda + 1)^2}{\lambda}$$

which implies that v is a square in $F_p^\times$ if and only if λ is a square as well. Now, suppose that t is not a square, so $SO(g_t) \simeq N$. If $\lambda = \mu^2$, with $\mu \in N$, then,

$$v = \frac{(\lambda + 1)^2}{\lambda} = \frac{(\mu^2 + 1)^2}{\mu^2} = \left(\frac{\mu^2 + 1}{\mu} \right)^2 = \left(\mu + \frac{1}{\mu} \right)^2,$$

and $\mu + \frac{1}{\mu} = \mu + \bar{\mu} = \mu + \mu^p = \text{Tr}(\mu) \in \mathbb{F}_p$, and so v is a square in $F_p^\times$.

Conversely, if $v = w^2$ is a square, then let μ be a square root of $\lambda \in \bar{\mathbb{F}}_p$. We need to show that $\mu \in N$. From the last equation, we get $w^2 = \left(\mu + \frac{1}{\mu} \right)^2$, and so $\mu + \frac{1}{\mu} = \pm w$.

Therefore, μ must satisfy the equation,

$$\mu^2 \pm w\mu + 1 = 0.$$

We know that we have:

$$(x - \mu)(x - \mu^p) = 0 \Leftrightarrow x^2 - \text{Tr}(\mu)x + N(\mu) = 0.$$

Thus, $\mu \in \mathbb{F}_p^2$ and μ has norm 1. It follows that $\mu \in N$, so λ is a square in N . $\square$

Recall that, if G is a group acting on a set X , the action is said to be **transitive** if, for all $x, y \in X$, it exists $g \in G$ such that $y = g \cdot x$. The action is **simply transitive** if g is unique.

Lemma 2.23. *Let $u \neq 0$ and let $D_{t,u}$ be the affine conic given by $x^2 - ty^2 = u$. The $SO(g_t)$ acts simply transitively on $D_{t,u}$.*

The proof is the same as the one in [CK15], with more detail.

Proof. The characteristic polynomial of $M_{\alpha,\beta}$ is $x^2 - 2\alpha x + 1$, so 1 is an eigenvalue if and only if $\alpha = 1$, in which case we have $\beta = 0$ (since $\alpha^2 - t\beta^2 = 1$), and so $M_{\alpha,\beta}$ is the identity matrix. Thus, no element of $SO(g_t)$ except the identity matrix can fix any nonzero vector. Note that if $M_{\alpha,\beta} \in SO(g_t)$ and $(x, y) \in D_{t,u}$, then

$$M_{\alpha,\beta} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha x + y\beta t \\ \beta x + \alpha y \end{pmatrix}$$

But,

$$(\alpha x + y\beta t)^2 - t(\beta x + \alpha y)^2 = (x^2 - ty^2)(\alpha^2 - t\beta^2) = u$$

Therefore, $SO(g_t)$ preserves $D_{t,u}$ and $|SO(g_t)| = |D_{t,u}|$, so it must act simply transitively. $\square$

Corollary 2.24. *Let $\psi \in SO(g_t)$ have characteristic polynomial $x^2 + (2-v)x + 1 = (x+1)^2 - vx$, with $v \neq 0$. Then, the sign of the permutation induced by ψ on $D_{t,u}$ is $\left(\frac{v}{p}\right)$.*

The subsequent proof is present in [CK15].

Proof. Let $k = \text{ord}(\psi)$ and $l = |SO(g_t)|/k$. Since $SO(g_t)$ is cyclic and its action on $D_{t,u}$ is simply transitive, the permutation induced by any generator of the group is a $|SO(g_t)|$ -cycle. Therefore, the permutation induced by ψ on $D_{t,u}$ is a product of l disjoint k -cycles, where $kl = |SO(g_t)| = p \pm 1$, which is even. Thus, the sign of the permutation is $(-1)^{(k+1)l} = (-1)^{kl+l} = (-1)^l$. By Proposition 2.22 this is equal to $\left(\frac{v}{p}\right)$. $\square$

We are now in conditions to analyze the cycle structure of the permutation τ_Q and show that its sign is $\left(\frac{q}{p}\right)$, proving the last part of Theorem 2.6, which we state again.

Theorem 2.25 (Cohn Kumar). *Let p and q be distinct primes with p odd. The sign of the permutation induced on the $p+1$ Hurwitz primes of norm p (up to left multiplication by units) through metacommutation by a prime of norm q is $\left(\frac{q}{p}\right)$.*

Like the proof of Theorem 2.18 we follow [CK15], with slight modifications.

Proof. We split the proof into various cases.

Case 1. $b = c = d = 0$.

In this case, τ_Q is the identity permutation, so it has $p+1$ fixed points. The sign of the permutation is then 1, which equals $\left(\frac{q}{p}\right)$ since $q = a^2$ is a square modulo p .

Case 2. $q = a^2$, but $(b, c, d) \neq 0$.

We know that τ_Q has exactly one fixed point on the conic C_p , so the remaining p points must permute. Also, the only eigenvalue of $\phi_{Q,p}$ is 1, which has multiplicity 3. Thus $N = \phi_{Q,p} - I$ has eigenvalue zero with multiplicity three, so it is nilpotent. In fact, by the Caley-Hamilton theorem,

$$N^3 = (\phi_{Q,p} - I)^3 = 0,$$

and since $p \geq 3$, $N^p = 0$. Then,

$$\phi_{Q,p}^p = (I + N)^p = I + N^p = I,$$

since we are in characteristic p . Therefore, the orbit sizes must all divide p , which forces the remain p points to be in one orbit, since p is prime. The permutation is thus a p -cycle, with sign $(-1)^{p+1} = 1$, which is again the same as $\left(\frac{q}{p}\right) = \left(\frac{a^2}{p}\right) = 1$.

For the remaining cases, let $v_0 = (b, c, d)$ be an eigenvector with eigenvalue 1 and nonzero norm ($b^2 + c^2 + d^2 \neq 0$). If $v = (x, y, z)$ is a vector on the cone K_p and orthogonal to v_0 , then

$$\begin{cases} bx + cy + dz = 0, \\ x^2 + y^2 + z^2 = 0. \end{cases}$$

As we saw in case 2 of the proof of Theorem 2.18, this system has zero or two solutions up to scaling. In the latter case, both are eigenvectors for $\phi_{Q,p}$ with eigenvalue -1 .

These fixed points have a null contribution to the sign of the permutation, so we only have to look at the orbits of the vectors that are not orthogonal to v_0 .

Then, if v is a vector on the cone K_p not orthogonal to v_0 , as we have already seen, there are $p \pm 1$ of these vectors up to scaling, depending on the number of fixed points. Then we may fix a scaling for v , by replacing it by $v/(v \cdot v_0)$. Therefore, we can assume that all these v satisfy $v \cdot v_0 = 1$. The linear transformation $\phi_{Q,p}$ permutes these vectors, and since if $v_0 \cdot v = 1$, one has

$$\phi_{Q,p}(v) \cdot v_0 = \phi_{Q,p}(v) \cdot \phi_{Q,p}(v_0) = v \cdot v_0 = 1.$$

For any such v , the projection along v_0 is the vector:

$$w_0 = \frac{v \cdot v_0}{v_0 \cdot v_0} v_0 = \frac{v_0}{v_0 \cdot v_0}.$$

Its projection orthogonal to v_0 is $v_\perp = v - w_0$. It is important to note that:

$$v_\perp \cdot v_\perp = v \cdot v - (w_0 \cdot w_0) = 0 - w_0 \cdot w_0 = -\frac{1}{v_0 \cdot v_0}.$$

Conversely, given any vector w of norm $\frac{-1}{v_0 \cdot v_0}$ orthogonal to v_0 , there is a unique vector v on the cone K_p with $v \cdot v_0 = 1$ and $v_\perp = w$, that is the vector, $v = w + w_0$. Thus, because v_0 is fixed, from the above arguments follows that $\phi_{Q,p}$ induces an orthogonal transformation on the orthogonal complement of v_0 .

Consider the usual quadratic form in $\mathbb{F}_p^3$, given by $Q(v) = v \cdot v = v\bar{v}$, let U be the subspace generated by v_0 and $U^\perp$ its orthogonal complement. Then from Lemma 1.86, follows that

$$\begin{aligned} \text{disc}(Q) &= \text{disc}(Q|_U) \times \text{disc}(Q|_{U^\perp}) \\ 1 &= (v_0 \cdot v_0) \times \text{disc}(Q|_{U^\perp}). \end{aligned}$$

Thus, this quadratic form on the orthogonal complement of v_0 has discriminant $\frac{1}{v_0 \cdot v_0}$, and so from Lemma 1.102 it must be equivalent to $f_Q(x, y) = x^2 - ty^2$, where $t = -\frac{1}{(v_0 \cdot v_0)} = (a^2 - q)^{-1}$.

Therefore, $\phi_{Q,p}$ gives rise to an element $\psi_Q \in SO_2(f_Q)$, whose characteristic polynomial is, by Lemma 2.17,

$$x^2 + 2 \left(1 - \frac{2a^2}{q}\right) x + 1,$$

since the quadratic form is in the subspace induced by $\phi_{Q,p}$ on the orthogonal complement of v_0 .

Thus, to understand the orbits of $\phi_{Q,p}$ on C_p it is enough to understand the action of ψ_Q on the vectors of norm $u = \frac{-1}{v_0 \cdot v_0}$ in $\mathbb{F}_p^2$.

Case 3. $a = 0$.

In this case, the characteristic polynomial is $x^2 + 2x + 1$ and so from the proof of Proposition 2.21, it follows that $\alpha = -1$ and $\beta = 0$, thus ψ_Q is given by the matrix:

$$M_{-1,0} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

which means that ψ_Q is the negation of the identity, so $\text{ord}(\psi) = 2$ and the permutation breaks up into a product of $(p \pm 1)/2$ disjoint transpositions. We have

$$\begin{aligned} \frac{1}{2} \left(p - \left(\frac{-q}{p} \right) \right) &= \frac{1}{2} \left(p - \left(\frac{-1}{p} \right) \right) + \frac{1}{2} \left(\frac{-1}{p} \right) \left(1 - \left(\frac{q}{p} \right) \right) \\ &\equiv \frac{1}{2} \left(1 - \left(\frac{q}{p} \right) \right) \pmod{2}, \end{aligned}$$

which is equal to $\left(\frac{q}{p} \right)$, thus the sign of the permutation is what we wanted.

Case 4. $a \neq 0$ and $a^2 \neq q$.

We apply Corollary 2.24 with $t = (a^2 - q)^{-1}$ and $v = \frac{4a^2}{q}$ to see that the sign of the permutation is the quadratic character of $\frac{4a^2}{q}$ modulo p which is precisely $\left(\frac{q}{p} \right)$.

□

Remark 2.26. It follows from the proof of the last theorem that if $a^2 = q$, modulo p , then there is only one fixed point and the remaining p primes are in one orbit. Thus the remaining permutation is a p -cycle.

As a consequence of the proof of Corollary 2.24, it follows from the proof of Theorem 2.25 that all the cycles which are not fixed points in the metacommutation map have the same length. Indeed, to understand the orbits of ϕ_Q on C_p , in the most general cases (3 and 4 of last theorem),

it is enough to understand the action of ψ_Q on the vectors of norm $u = \frac{1}{v_0 \cdot v_0}$. Thus, in the proof of Corollary 2.24 we saw that the permutation induced by ψ_Q is a product of $\frac{|SO(g_t)|}{\text{ord}(\psi_Q)}$ disjoint $\text{ord}(\psi_Q)$ -cycles. The other cases are either the identity or the case of Remark 2.26. Therefore, we have that:

Theorem 2.27. *All of the cycles which are not fixed points in the metacommutation map have the same length.*

This result is also proved in Theorem 5.3 of [FGS15] using the fact that we can perceive the metacommutation map as a group action on the projective line over $\mathbb{F}_p$.

This theorem implies that the cycle length divides $p + 1$, p or $p - 1$ depending whether the permutation has respectively 0, 1 or 2 fixed points.

Chapter 3

On the cycle structure of the Metacommutation map

As a consequence of Theorem 2.27 we know that the permutation induced in the non-fixed points must be a product of disjoint cycles of the same length. We call **non-trivial cycles** to all these cycles. Recall that Theorem 2.6 implies that assuming the existence of non-trivial cycles is the same as saying that $\tau_{Q,p}$ cannot be the identity, thus p must be odd and Q must not be congruent to an integer modulo p . In his PhD thesis, [Tso20], Nikolaos Tsopanidis gives criteria to decide when the non-trivial cycles are of length 2 or 3.

Proposition 3.1. *The non-trivial cycles of $\tau_{Q,p}$ have length 2 if and only if Q is pure modulo p , and they have length 3 if and only if $N(Q) \equiv \text{Tr}(Q)^2 \pmod{p}$.*

Proof. See the proofs of Proposition 5.4 and Proposition 5.5 in [Tso20]. □

Using these results as a baseline, and results present in Chapter 2, in this section we prove new criteria to decide when the non-trivial cycles are of length 4 or 6, and analyze $\tau_{Q,p}$ in the case of cycles of length 4. Then, we generalize our results to all lengths, giving us a faster way to decide when the non-trivial cycles have arbitrary length $\ell \in \mathbb{N}$.

3.1 Cycles of length 4 and 6

We start this section with a lemma that is useful to prove the criteria to decide whether the non-trivial cycles are of length 4 or 6. We assume that p is odd and that Q is not congruent to an integer modulo p .

Lemma 3.2. *The conic $C_p = \{[x : y : z] \in \mathbb{P}^2(\mathbb{F}_p) \mid x^2 + y^2 + z^2 = 0\}$ has three linear independent vectors.*

This proof derives from the proof of Proposition 5.4 in [Tso20].

Proof. First choose $a, b \in \mathbb{F}_p$ such that $a^2 + b^2 + 1 = 0$, modulo p , which we have seen that is possible in the proof of Proposition 2.7. Notice that $(1, a, b)$, $(b, 1, a)$ and $(a, b, 1)$ are 3 distinct

points in C_p . Consider the matrix A which has these vectors as columns,

$$A = \begin{pmatrix} 1 & b & a \\ a & 1 & b \\ b & a & 1 \end{pmatrix}.$$

This matrix has determinant $\det(A) = a^3 + b^3 - 3ab + 1$. If we consider the vectors $(1, a, b)$, $(b, -1, a)$ and $(a, b, -1)$, that are also in C_p , then we have

$$B = \begin{pmatrix} 1 & b & a \\ a & -1 & b \\ b & a & -1 \end{pmatrix},$$

and $\det(B) = a^3 + b^3 + ab + 1$. Then, at least one of the determinants is nonzero in $\mathbb{F}_p$. In fact, if $\det(A) = \det(B) = 0$, modulo p , then $4ab = 0$, and so, modulo p , either $a = 0$ or $b = 0$. We can assume, without loss of generality, that $b = 0$. Then $a^2 + 1 = 0$ (thus $a \neq 0$) and, since $\det(A) = 0$, we also have that $a^3 + 1 = 0$. Thus, $a^3 = a^2$, and so $a = 1$. But, from $a^2 + 1 = 0$ we have that $2 = 0$, which is a contradiction. □

Proposition 3.3. *The non trivial cycles of $\tau_{Q,p}$ have length 4 if and only if*

$$2N(Q) \equiv \text{Tr}(Q)^2 \pmod{p}.$$

Proof. Let $Q \equiv a + bi + cj + dk \pmod{p}$ and $N(Q) = q$. From Chapter 2, we know that we can think of $\tau_{Q,p}$ as the left action of the matrix

$$\phi_{Q,p} = \frac{1}{q} \begin{pmatrix} a^2 + b^2 - c^2 - d^2 & 2ad + 2bc & -2ac + 2bd \\ -2ad + 2bc & a^2 - b^2 + c^2 - d^2 & 2ab + 2cd \\ 2ac + 2bd & -2ab + 2cd & a^2 - b^2 - c^2 + d^2 \end{pmatrix},$$

on the points of the conic C_p . If $2N(Q) \equiv \text{Tr}(Q)^2 \pmod{p}$, then one has,

$$2q \equiv 4a^2 \pmod{p} \Leftrightarrow q \equiv 2a^2 \pmod{p} \Leftrightarrow b^2 + c^2 + d^2 \equiv a^2 \pmod{p}.$$

Since $\text{Tr}(\phi_{Q,p}) = \frac{4a^2}{q} - 1$, it follows that,

$$\text{Tr}(\phi_{Q,p}) \equiv \frac{4a^2}{q} - 1 \equiv \frac{3a^2 - (b^2 + c^2 + d^2)}{q} \equiv \frac{2a^2}{q} \equiv 1 \pmod{p}.$$

From the fact that $\phi_{Q,p}$ satisfies its characteristic polynomial, we get that

$$\phi_{Q,p}^3 - \text{Tr}(\phi_{Q,p})\phi_{Q,p}^2 + \text{Tr}(\phi_{Q,p})\phi_{Q,p} - I = 0.$$

Therefore, in $\mathbb{F}_p$, $\phi_{Q,p}^3 - \phi_{Q,p}^2 + \phi_{Q,p} - I = 0 \Leftrightarrow \phi_{Q,p}^3 = \phi_{Q,p}^2 - \phi_{Q,p} + I$. Immediately, we get that $\phi_{Q,p}^4 = \phi_{Q,p}^3 - \phi_{Q,p}^2 + \phi_{Q,p} = I$, so $\phi_{Q,p}^4 = I$, in $\mathbb{F}_p$.

We know that all the non-trivial cycles have the same length. If this length were equal to 3, then we would have $\phi_Q^3 = I$, which implies that $\phi_{Q,p} = I$. It would mean that there is no cycle with length greater than one, which is a contradiction. If the length were equal to 2, then $\phi_Q^2 = I$, so $\phi_{Q,p}^3 = \phi_{Q,p} \circ \phi_{Q,p}^2 = \phi_{Q,p}$. From $\phi_{Q,p}^3 - \phi_Q^2 + \phi_{Q,p} - I = 0$ we get that $\phi_{Q,p} - I + \phi_{Q,p} - I = 0 \Leftrightarrow 2\phi_{Q,p} = 2I \Leftrightarrow \phi_{Q,p} = I$ and, again, we get a contradiction. We conclude that all the non-trivial cycles have length 4.

Conversly, if the non-trivial cycles of $\tau_{Q,p}$ have length 4, then $\phi_{Q,p}^4$ fixes every point of C_p . Therefore, since we know from Lemma 3.2 that there are 3 linearly independent vectors in C_p , $\phi_{Q,p}^4$ is the identity operator, i.e., $\phi_{Q,p}^4 = I$ in $\mathbb{F}_p$. This means that

$$\phi_{Q,p}^4 - I = 0 \Leftrightarrow (\phi_{Q,p}^2 + I)(\phi_{Q,p}^2 - I) = 0.$$

Therefore, either $\phi_{Q,p}^2 = -I$ or $\phi_{Q,p}^2 = I$, but we cannot have the latter since that would mean that all non trivial cycles oh $\tau_{Q,p}$ have length 2 which is a contradiction. Thus, we should have $\phi_{Q,p}^2 = -I$, so $\phi_{Q,p}^3 = -\phi_{Q,p}$. Using again the fact that $\phi_{Q,p}$ satisfies its characteristic polynomial, we conclude that, in $\mathbb{F}_p$,

$$\begin{aligned} \phi_{Q,p}^3 - \text{Tr}(\phi_{Q,p})\phi_{Q,p}^2 + \text{Tr}(\phi_{Q,p})\phi_{Q,p} - I &= 0 \\ \Leftrightarrow -\phi_{Q,p} + \text{Tr}(\phi_{Q,p})I + \text{Tr}(\phi_{Q,p})\phi_{Q,p} - I &= 0 \\ \Leftrightarrow (\text{Tr}(\phi_{Q,p}) - 1)(\phi_{Q,p} + I) &= 0. \end{aligned}$$

Therefore, either $\phi_{Q,p} = -I$ or $\text{Tr}(\phi_{Q,p}) = 1$ in $\mathbb{F}_p$. If $\phi_{Q,p} = -I$, we have a clear contradiction, so $\text{Tr}(\phi_{Q,p}) \equiv 1 \pmod{p}$, and since $\text{Tr}(\phi_{Q,p}) = \frac{4a^2}{q} - 1$, we get that $4a^2 \equiv 2q \pmod{p}$, meaning that $\text{Tr}(Q)^2 \equiv 2N(Q) \pmod{p}$.

□

Proposition 3.3 says that for an odd prime p , and $Q = a + bi + cj + dk$, modulo p , the non-trivial cycles of $\tau_{Q,p}$ have length 4 if and only if $2N(Q) = \text{Tr}(Q)^2$, which is the same as saying that $2a^2 = q$. From Theorem 2.18, the number of fixed points is given by $1 + \left(\frac{a^2 - q}{p}\right)$, thus if the non trivial cycles have length 4, the number of fixed points is $1 + \left(\frac{-a^2}{p}\right) = 1 + \left(\frac{-1}{p}\right)$.

Therefore, if the non-trivial cycles have length 4 (that is if $2a^2 = q$), the number of fixed points does not depend on the quadratic character of $a^2 - q$, but simply on the quadratic character of $-1 \pmod{p}$. Notice, that -1 is a quadratic residue if $p \equiv 1 \pmod{4}$ and a quadratic non-residue if $p \equiv 3 \pmod{4}$. This means that we have two fixed points if $4 \mid (p - 1)$ and we do not have fixed points if $4 \mid (p + 1)$. Thus, for the primes p of the form $4k + 1$, the permutation consists of 2 fixed points and $(p - 1)/4$ cycles of length 4, and for the primes of the form $4k + 3$ the permutation consists of $(p + 1)/4$ cycles of length 4. Recall that from Theorem 2.27, we already knew that the length of the non-trivial cycles divides $p + 1, p$ or $p - 1$, depending on the number of fixed points.

Example 3.4. Imagine that we have $p = 7$, then $4 \mid p + 1$. So from the above discussion, if we have non-trivial cycles of length 4, we cannot have fixed points. As a particular example, if $Q = 3 + i + j$, then $q = 11$, and we have $2 \times 3^2 = 18 = 11$, modulo 7, and the permutation $\tau_{Q,p}$ consists of 2 cycles of length 4.

One can go one step further and compute, with the help of SageMath, all the pairs (a^2, q) such that $2a^2 = q$, modulo p . The following code does exactly that for the first 350 primes,

```

1 Gp()
2 from math import *
3 Primes=gp.Set(gp.primes(350))
4
5 def PossQ(p):
6     a=[]
7     Q=[]
8     for i in range(1,int((p+1)/2)):
9         a.append(i**2)
10    for i in range(int((p-1)/2)):
11        R=[]
12        for q in range(1,351):
13            if (a[i] < Primes[q]) and (2*a[i])%p==Primes[q]%p:
14                R.append(Primes[q])
15        Q.append(R)
16    for i in range(int((p-1)/2)):
17        print ("a^2= " + str(a[i]%p))
18        print (str(Q[i])+"\n")

```

In the case $p = 7$ it yields:

```

1 a^2= 1
2 [2, 23, 37, 79, 107, 149, 163, 191, 233, 317, 331, 359, 373, 401, 443, 457,
3 499, 541, 569, 653, 709, 751, 821, 863, 877, 919, 947, 1031, 1087, 1129, 1171,
4 1213, 1283, 1297, 1367, 1381, 1409, 1423, 1451, 1493, 1549, 1619, 1759, 1787,
5 1801, 1871, 1913, 1997, 2011, 2039, 2053, 2081, 2137, 2179, 2207, 2221, 2333,
6 2347]
7
8 a^2= 4
9 [29, 43, 71, 113, 127, 197, 211, 239, 281, 337, 379, 421, 449, 463, 491, 547,
10 617, 631, 659, 673, 701, 743, 757, 827, 883, 911, 953, 967, 1009, 1051, 1093,
11 1163, 1289, 1303, 1373, 1429, 1471, 1499, 1583, 1597, 1667, 1709, 1723, 1877,
12 1933, 2003, 2017, 2087, 2129, 2143, 2213, 2269, 2297, 2311, 2339]
13
14 a^2= 2
15 [11, 53, 67, 109, 137, 151, 179, 193, 263, 277, 347, 389, 431, 487, 557, 571,
16 599, 613, 641, 683, 739, 809, 823, 907, 977, 991, 1019, 1033, 1061, 1103, 1117,
17 1187, 1201, 1229, 1327, 1439, 1453, 1481, 1523, 1579, 1607, 1621, 1663, 1733,
18 1747, 1789, 1831, 1873, 1901, 1999, 2027, 2069, 2083, 2111, 2153, 2237, 2251,
19 2293]

```

One should note that the code obviously does not imply that all quaternions with norm q work. For example, considering $q = 107$, we have that, for the quaternion $Q = 7 + 3i + 7j$, the permutation consists in 4 cycles of length 2, as we already knew from Proposition 3.1. We only know that if such Q exists then its norm must be on the above list (for the first 350 primes). However, we still need to obey to the equation $2a^2 = q$. To explicitly find a quaternion Q such that the length of the non-trivial cycles is 4, consider the following code, where all the auxiliary functions are defined in Appendix B.

```

1 def GivenQ(p,Q,a):
2     V=gp.PrimosT(Q)
3     x=[]
4     for j in range(1,len(V)+1):
5         B=gp.AllLassoc(gp.quat(V[j][1],V[j][2],V[j][3],V[j][4]))
6         for k in range(1, len(B)+1):
7             C=list(B[k])
8             for i in range(4):
9                 if a==(C[i]*C[i])%p:
10                     b=C[i]
11                     C.remove(C[i])
12                     C.insert(0,b)
13                     if C not in x:
14                         x.append(C)
15     return x

```

Thus, if we compute, for example, $\text{GivenQ}(7,11,2)$, we get a list of quaternions in which we recover the quaternion $3 + i + j$ from the Example 3.4.

Remark 3.5. If we have a $Q = a + bi + cj + dk$, such that $2a^2 = q$ modulo p , then all the quaternions $\{\pm a \pm bi \pm cj \pm dk\}$ will also give us a permutation in which the non-trivial cycles have length 4. Additionally, one can change the position of the integers b, c and d at will, since our conditions depend only on a and q . Thus, the above function returns a list in which most of the quaternions are essentially the same.

Analyzing the results of Nikolaos and Proposition 3.3, one could wonder what happens when $3N(Q) = \text{Tr}(Q)^2$, modulo p . In fact, this gives us exactly a criteria to decide when we have non-trivial cycles of length 6.

Proposition 3.6. *The non-trivial cycles of $\tau_{Q,p}$ have length 6 if and only if*

$$3N(Q) \equiv \text{Tr}(Q)^2 \pmod{p}.$$

Proof. Let $Q \equiv a + bi + cj + dk \pmod{p}$, $N(Q) = q$, and $\phi_{Q,p}$, the matrix given in the proof of Proposition 3.3. If $3N(Q) \equiv \text{Tr}(Q)^2 \pmod{p}$, then $4a^2 \equiv 3q \pmod{p}$ and we have,

$$\text{Tr}(\phi_{Q,p}) \equiv \frac{4a^2}{q} - 1 \equiv \frac{3q - q}{q} \equiv 2 \pmod{p}.$$

Again, since $\phi_{Q,p}$ satisfies its characteristic polynomial we have that,

$$\phi_{Q,p}^3 - \text{Tr}(\phi_{Q,p})\phi_{Q,p}^2 + \text{Tr}(\phi_{Q,p})\phi_{Q,p} - I = 0.$$

Therefore, in $\mathbb{F}_p$, $\phi_{Q,p}^3 - 2\phi_{Q,p}^2 + 2\phi_{Q,p} = I \Leftrightarrow \phi_{Q,p}^3 - I = 2\phi_{Q,p}^2 - 2\phi_{Q,p}$.

Since $\phi_{Q,p}$ cannot be the identity, because that would imply that all cycles have length 1, it follows that,

$$\phi_{Q,p}^3 - I = 2\phi_{Q,p}(\phi_{Q,p} - I) \Leftrightarrow \phi_{Q,p}^2 + \phi_{Q,p} + I = 2\phi_{Q,p} \Leftrightarrow \phi_{Q,p}^2 - \phi_{Q,p} + I = 0.$$

We get $\phi_{Q,p}^2 - \phi_{Q,p} + I = 0$ which is a divisor of $\phi_{Q,p}^6 - I = 0$, so $\phi_{Q,p}^6 = I$. In fact, the polynomial $x^2 - x + 1 = 0$ is the 6th cyclotomic polynomial, in $\mathbb{F}_p$, so $\phi_{Q,p}^d \neq I$ for all $d < 6$. Therefore, we must have that all non-trivial cycles have length 6.

Conversly, if the non-trivial cycles of $\tau_{Q,p}$ have length 6, then $\phi_{Q,p}^6$ fixes every point of C_p , thus, since, from Lemma 3.2, there are 3 linearly independent vectors in C_p , $\phi_{Q,p}^6$ is the identity operator, i.e., $\phi_Q^6 = I$ in $\mathbb{F}_p$. Thus,

$$\phi_{Q,p}^6 - I = 0 \Leftrightarrow (\phi_{Q,p}^3 - I)(\phi_{Q,p}^3 + I) = 0.$$

So, either $\phi_{Q,p}^3 - I = 0$ or $\phi_{Q,p}^3 + I = 0$. We cannot have the first one, since it would mean that we have cycles with length different than 6, which is a contradiction. Thus, we must have $\phi_{Q,p}^3 + I = 0$, so

$$(\phi_{Q,p} + I)(\phi_{Q,p}^2 - \phi_{Q,p} + I) = 0.$$

If we had that $\phi_{Q,p} + I = 0 \Leftrightarrow \phi_{Q,p} = -I$, then $\phi_{Q,p}^2 = I$, and as before we get a contradiction. Therefore, we must have $\phi_{Q,p}^2 - \phi_{Q,p} + I = 0$. Since $\phi_{Q,p}$ satisfies its characteristic polynomial, we have again

$$\phi_{Q,p}^3 - \text{Tr}(\phi_{Q,p})\phi_{Q,p}^2 + \text{Tr}(\phi_{Q,p})\phi_{Q,p} - I = 0,$$

which is equivalent to,

$$(\phi_{Q,p} - I)(\phi_{Q,p}^2 + (1 - \text{Tr}(\phi_{Q,p}))\phi_{Q,p} + I) = 0.$$

Since we cannot have $\phi_{Q,p} = I$, we must have that $\phi_{Q,p}^2 + (1 - \text{Tr}(\phi_{Q,p}))\phi_{Q,p} + I = 0$ and using the fact that $\phi_{Q,p}^2 - \phi_{Q,p} + I = 0$, we must have, in $\mathbb{F}_p$,

$$1 - \text{Tr}(\phi_{Q,p}) = -1 \Leftrightarrow \text{Tr}(\phi_{Q,p}) = 2,$$

and from $\text{Tr}(\phi_{Q,p}) = \frac{4a^2}{q} - 1$, we get $4a^2 \equiv 3q \pmod{p}$, meaning $\text{Tr}(Q)^2 \equiv 3N(Q) \pmod{p}$. □

3.2 A generalization

We are now in position to generalize our results to all possible lengths. Notice that in the proof of the last two propositions, appears a certain type of polynomials which we introduced in Section 1.2.3, that are the cyclotomic polynomials. In the next theorem, we see that, in fact, there is a relation between this polynomials and the characteristic polynomial of $\phi_{Q,p}$. Given an odd rational prime p , a prime quaternion Q , not congruent to a rational integer modulo p , and $\ell \in \mathbb{N}$, the following theorem provides a necessary and sufficient condition for the non-trivial cycles of $\tau_{Q,p}$ to have length ℓ .

Theorem 3.7. *Let p be an odd prime, Q a Hurwitz prime not congruent to a rational integer modulo p , and let $\ell_{Q,p}$ be the length of non-trivial cycles of $\tau_{Q,p}$. Then $\ell_{Q,p} = t$ if and only if $(f_Q(x), \Phi_t(x)) \neq 1$, where $f_Q(x) = x^2 + 2\left(1 - \frac{2a^2}{q}\right)x + 1$ and $\Phi_t(x)$ is the t^{th} cyclotomic polynomial, over $\mathbb{F}_p$.*

Proof. Let $Q \equiv a + bi + cj + dk \pmod{p}$ and $N(Q) = q$. Since p is odd and Q is not congruent to an integer modulo p , the metacommutation map $\tau_{Q,p}$ has non-trivial cycles.

We know, from our earlier discussion, that we can think of $\tau_{Q,p}$ as the left action of the matrix

$$\phi_{Q,p} = \frac{1}{q} \begin{pmatrix} a^2 + b^2 - c^2 - d^2 & 2ad + 2bc & -2ac + 2bd \\ -2ad + 2bc & a^2 - b^2 + c^2 - d^2 & 2ab + 2cd \\ 2ac + 2bd & -2ab + 2cd & a^2 - b^2 - c^2 + d^2 \end{pmatrix},$$

on the points of the conic $C_p = \{[x : y : z] \in \mathbb{P}^2(\mathbb{F}_p) \mid x^2 + y^2 + z^2 = 0\}$. If the non-trivial cycles have length $\ell_{Q,p} = t$, then $\phi_{Q,p}^t$ fixes every point of the conic C_p , and therefore it must be the identity operator. In other words, we must have $\phi_{Q,p}^t = I$ and $\phi_{Q,p}^d \neq I$, $\forall d \in \{1, \dots, n\}$.

In the case $\ell_{Q,p} = p$, then the metacommutation map $\tau_{Q,p}$ has only one fixed point and, from Theorem 2.18, $a^2 = q$, which means that $f_Q(x) = (x-1)^2$. The p^{th} cyclotomic polynomial over $\mathbb{F}_p$ is simply $(x-1)^{p-1}$, so $(f_Q(x), \Phi_p(x)) \neq 1$. If $(f_Q(x), \Phi_p(x)) \neq 1$, then $(x-1)$ must divide f_Q and we get that $a^2 = q$. Thus there is only one fixed point and a cycle of length p , so $\ell_{Q,p} = p$.

In the case $\ell_{Q,p} \mid p \pm 1$, p does not divide $\ell_{Q,p} = t$, so from the Theorem 1.75, the polynomial $x^t - 1$ can be written as $x^t - 1 = \prod_{d \mid t} \Phi_d(x)$, where $\Phi_d(x)$ is the d^{th} cyclotomic polynomial over $\mathbb{F}_p$. We have that $\phi_{Q,p}$ satisfies the polynomial $x^t - I = 0$, so $\prod_{d \mid t} \Phi_d(\phi_{Q,p}) = 0$. Therefore, we must have $\Phi_t(\phi_{Q,p}) = 0$, since $\Phi_d(\phi_{Q,p}) \neq 0 \forall d < t$. From the fact that $(x-1)f_Q(x)$ is the characteristic polynomial of $\phi_{Q,p}$, one must also have that $f_Q(\phi_{Q,p}) = 0$. Thus, $\Phi_t(\phi_{Q,p}) = 0$ and $f_Q(\phi_{Q,p}) = 0$. If $g(x)f_Q(x) + h(x)\Phi_t(x) = 1$, then that implies $g(\phi_{Q,p})f_Q(\phi_{Q,p}) + h(\phi_{Q,p})\Phi_t(\phi_{Q,p}) = I$, so $0 = I$, which is a contradiction.

For the other implication, let $(f_Q, \Phi_t) \neq 1$, then exists $\lambda \in \bar{\mathbb{F}}_p^\times$ such that $f_Q(\lambda) = \Phi_t(\lambda) = 0$. Therefore, since λ it satisfies the t^{th} cyclotomic polynomial, $\lambda^t = 1$ and $\lambda^d \neq 1 \forall d < t$, which implies that its order is t . Since f_Q is the characteristic polynomial of an element $\psi_Q \in SO_2(g_t)$, and we know, that from Proposition 2.21, ψ_Q is semisimple, its order is equal to the order of λ , so it is also t . Also, as a consequence of the proof of Theorem 2.25, in order to understand the orbits of $\phi_{Q,p}$ on C_p it is enough to understand the action of ψ_Q on elements of a fixed norm, which we know is cyclic and, as we have seen, has order t . Therefore, the orbits of $\phi_{Q,p}$ which are not fixed points must all have order t , i.e., the non-trivial cycles must all have order t . Hence, $\phi_{Q,p}^t = 1$ and $\ell_{Q,p} = t$. $\square$

From Remark 1.59, we know that f_Q and Φ_t will have a common divisor in $\mathbb{F}_p$ if and only if $R(f_Q, \Phi_t) = 0$, and therefore we have a easier way of knowing if $\ell_{Q,p} = t$. For example, imagine that we want to have a Q such that $\ell_{Q,p} = 5$, then computing the resultant of f_Q and Φ_5 , gets us $(4\alpha^2 + 2\alpha - 1)^2 = 0$, where $\alpha = (1 - \frac{2a^2}{q})$. Then, if we adapt the code we made earlier for the case of cycles of length 4, we can easily find a Q under these conditions.

For an odd p prime, we have, from the previous theorem, that $\ell_{Q,p} = 4$ if and only if $(f_Q(x), \Phi_4(x)) \neq 1$, which only happens when $2\left(1 - \frac{2a^2}{q}\right) = 0 \Leftrightarrow 2a^2 = q$, modulo p , which gives us the same result we had in Proposition 3.3. In fact, we have that $2a^2 = q$ implies $f_Q = x^2 + 1$, which is equal to $\Phi_4(x)$. So, for example, if $p = 13$, and $Q = 3 + 3i - 3j - 2k$, then $q = 31$, and $2 \times 3^2 \equiv 31$ modulo 13, and $\tau_{Q,p}$ has two fixed points and 3 cycles of length 4.

Now, if we want we want to decide when the non-trivial cycles are of length 2, then $(f_Q(x), \Phi_2(x)) \neq 1$, which is equivalent to $2 - 2\left(1 - \frac{2a^2}{q}\right) = 0 \Leftrightarrow a = 0$, and so we get the same

result as in [Tso20].

3.3 Common left and right-hand divisors of a quaternion integer

The results of last section provide us a criterion to decide when the non-trivial cycles have a determined length. Imagine now that we have a particular prime quaternion P with norm p , a rational odd prime. One may speculate which primes Q yield a permutation $\tau_{Q,p}$, such that P is a fixed point. Recall that P is a fixed point of $\tau_{Q,p}$, then, up to unit-migrations, we have $\alpha = PQ = Q'P$, for some prime Q' . Thus, P is a common left and right-hand divisor of α . This motivates us to first study the results present in [AADGS13], which gives the conditions under which a quaternion integer has common left- and right-hand divisors.

Let α be a primitive quaternion in $\mathcal{H}$ whose norm is divisible by a positive integer m . We would like to know whether α has any common left and right-hand factors of norm m . That is, if exist β, γ and γ' in $\mathcal{H}$ such that $N(\beta) = m$ and $\alpha = \beta\gamma = \gamma'\beta$. If we define the sets:

$$L_m(\alpha) = \{\beta \in \mathcal{H} \mid \alpha = \beta\gamma \text{ with } \gamma \in \mathcal{H} \text{ and } N(\beta) = m\},$$

and

$$R_m(\alpha) = \{\beta \in \mathcal{H} \mid \alpha = \gamma'\beta \text{ with } \gamma' \in \mathcal{H} \text{ and } N(\beta) = m\},$$

as the sets of left- and right-hand factors of α with norm m , then our main problem is determining:

$$L_m(\alpha) \cap R_m(\alpha),$$

for a given α and $m \mid N(\alpha)$. Before we move on, we make the following distinction,

Definition 3.8. Let $\alpha \in \mathcal{H}$. Then α is of **type (I)** if $\alpha \in \mathcal{L}$. Otherwise is of **type (II)**.

For any element $\alpha = a_0 + a_1i + a_2j + a_3k \in \mathcal{H}$, we set $a'_i = a_i$ if α has type (I) and $a'_i = 2a_i$ if α is type (II).

Theorem 3.9. Suppose that $\alpha = a_0 + a_1i + a_2j + a_3k \in \mathcal{H}$ is primitive and let m be an odd integer such that $m \mid N(\alpha)$. Then,

$$L_m(\alpha) \cap R_m(\alpha) \neq \emptyset$$

if and only if there exists $\beta = b_0 + b_1i + b_2j + b_3k \in \mathcal{H}$ such that $N(\beta) = m$ and $a'_ib'_j \equiv a'_jb'_i \pmod{m}$, for all $i \neq j$. Moreover, $\beta \in L_m(\alpha) \cap R_m(\alpha)$.

Throughout this proof we follow the work contained in [AADGS13].

Proof. If we assume that $L_m(\alpha) \cap R_m(\alpha) \neq \emptyset$, then there must exist quaternions $\beta, \gamma, \gamma' \in \mathcal{H}$ such that $N(\beta) = m$ and $\alpha = \beta\gamma = \gamma'\beta$. Therefore, $\gamma' = \beta\gamma\beta^{-1} \in \mathcal{H}$ and we can compute its coordinates. First, see that

$$\Re(\gamma') = \gamma' \cdot 1 = \beta\gamma\beta^{-1} \cdot 1 = \beta\gamma \cdot \overline{\beta^{-1}} = \frac{1}{N(\beta)}(\beta\gamma \cdot \beta) = \frac{1}{N(\beta)}N(\beta)(\gamma \cdot 1) = \gamma \cdot 1 = \Re(\gamma), \quad (3.1)$$

and so γ and γ' are both of type (I) or both of type (II). Then, we compute:

$$\gamma' \cdot i = \beta\gamma\beta^{-1} \cdot i = \frac{1}{N(\beta)}(\beta\gamma \cdot i\beta).$$

Since $i\beta = -b_1 + b_0i - b_3k + b_2k$ and $\beta i = -b_1 + b_0i + b_3j - b_2k$, we have $i\beta = \beta i - 2b_3j + 2b_2k$.

Thus,

$$\begin{aligned} \gamma' \cdot i &= \frac{1}{N(\beta)}(\beta\gamma \cdot \beta i - 2b_3 + 2b_2k) \\ &= \frac{1}{N(\beta)}(\beta\gamma \cdot \beta i) + \frac{1}{N(\beta)}(\beta\gamma \cdot -2b_3j + 2b_2k) \\ &= (\gamma \cdot i) + \frac{1}{N(\beta)}(\alpha \cdot -2b_3j + 2b_2k) \\ &= (\gamma \cdot i) + \frac{1}{N(\beta)}(a_0 + a_1i + a_2j + a_3k \cdot -2b_3j + 2b_2k) \\ &= (\gamma \cdot i) + \frac{1}{N(\beta)}(-2a_2b_3 + 2a_3b_2). \end{aligned}$$

Since both γ and γ' are of the same type we have $(\gamma' \cdot i) - (\gamma \cdot i) \in \mathbb{Z}$, so it must follow that

$$\frac{2}{m}(-a_2b_3 + a_3b_2) \in \mathbb{Z}.$$

Since $\gcd(2, m) = 1$, one can check that regardless of the types of α and β , $a'_2b'_3 \equiv a'_3b'_2 \pmod{m}$.

Similar calculations yield,

$$\gamma' \cdot j = \gamma \cdot j + \frac{2}{m}(-a_3b_1 + a_1b_3),$$

and

$$\gamma' \cdot k = \gamma \cdot k + \frac{2}{m}(-a_1b_2 + a_2b_1).$$

This implies, $a'_1b'_3 \equiv a'_3b'_1 \pmod{m}$ and $a'_1b'_2 \equiv a'_2b'_1 \pmod{m}$. To get the other three conditions of the theorem, we compute

$$\begin{aligned} 2(\gamma' \cdot i) &= 2(\alpha\beta^{-1} \cdot i) = \frac{2}{N(\beta)}(\alpha\bar{\beta} \cdot i) = \frac{2}{m}(-a_0b_1 + a_1b_0 - a_2b_3 + a_3b_2) \\ 2(\gamma' \cdot j) &= 2(\alpha\beta^{-1} \cdot j) = \frac{2}{N(\beta)}(\alpha\bar{\beta} \cdot j) = \frac{2}{m}(-a_0b_2 + a_2b_0 + a_1b_3 - a_3b_1) \\ 2(\gamma' \cdot k) &= 2(\alpha\beta^{-1} \cdot k) = \frac{2}{N(\beta)}(\alpha\bar{\beta} \cdot k) = \frac{2}{m}(-a_0b_3 + a_3b_0 - a_1b_2 + a_2b_1) \end{aligned}$$

In the final expression of each equation, the numerator of the sum of the final two terms is divisible by m , as we discovered from the previous conditions. Thus, the same must be true for the sum of the first two terms, leading us to

$$a'_0b'_1 \equiv a'_1b'_0 \pmod{m}, \quad a'_0b'_2 \equiv a'_2b'_0 \pmod{m}, \quad a'_0b'_3 \equiv a'_3b'_0 \pmod{m}.$$

For the other direction, suppose we have $N(\beta) = m$ such that $a'_ib'_j \equiv a'_jb'_i \pmod{m}$ for all $i \neq j$. We need to show that β divides α on the left and right, which is the same as showing that $\gamma' = \alpha\beta^{-1}$ and $\gamma = \beta^{-1}\alpha$ are in $\mathcal{H}$. The previous expressions for $2(\gamma' \cdot i)$, $2(\gamma' \cdot j)$ and $2(\gamma' \cdot k)$, together with the assumptions $a'_ib'_j \equiv a'_jb'_i \pmod{m}$, imply that each of $(\gamma' \cdot i)$, $(\gamma' \cdot j)$ and $(\gamma' \cdot k)$

is in $\frac{1}{4}\mathbb{Z}$. This is due to the fact that four corresponding terms $a_i b_j$ are in $\frac{1}{4}\mathbb{Z}$. Additionally, if one of the four terms $a_i b_j$ is not in $\frac{1}{2}\mathbb{Z}$, then $\alpha, \beta \in \mathcal{H} \setminus \mathcal{L}$ and so none of the other three are in $\frac{1}{2}\mathbb{Z}$. In any case, we have that $\gamma' \cdot i, \gamma' \cdot j$ and $\gamma' \cdot k$ is in fact in $\frac{1}{2}\mathbb{Z}$. It remains to notice that the equation,

$$(\gamma' \cdot 1)^2 + (\gamma' \cdot i)^2 + (\gamma' \cdot j)^2 + (\gamma' \cdot k)^2 = N(\gamma') \in \mathbb{Z},$$

implies that $\gamma' \cdot 1 \in \frac{1}{2}\mathbb{Z}$, with all of $\gamma' \cdot 1, \gamma' \cdot i, \gamma' \cdot j$ and $\gamma' \cdot k$ in $\mathbb{Z}$ or all in $\mathbb{Z} + \frac{1}{2}$. We conclude that $\gamma' \in \mathcal{H}$, and a similar calculation shows that $\gamma \in \mathcal{H}$. □

Remark 3.10. In the proof above, we proved in equation 3.1 that if two quaternions are conjugates, then their real part is the same.

3.3.1 Fixed points revisited

Now that we have established Theorem 3.9, we can look at it from the point of view that most interest us. For instance, consider a primitive quaternion α whose norm is $N(\alpha) = pq$, where p is an odd rational prime. Then, by Theorem 1.20, there is a factorization $\alpha = PQ$, modeled on pq . It follows from Theorem 2.18 that, if $\tau_{Q,p}$ is not the identity, the number of fixed points of $\tau_{Q,p}$ is $1 + \left(\frac{a^2 - q}{p}\right)$. If P is a fixed point of the metacommutation map, up to unit-migration, then $\alpha = PQ = Q'P$. Thus, we have that

$$P \in L_m(\alpha) \cap R_m(\alpha).$$

Therefore, with the help of the Theorem 3.9, we can establish the following corollary,

Corollary 3.11. *Let $\alpha = a_0 + a_1i + a_2j + a_3k$ be primitive such that $N(\alpha) = pq$, with p an odd prime. Then $P = b_0 + b_1i + b_2j + b_3k \in \mathcal{H}$ is a fixed point of $\tau_{Q,p}$ if and only if $N(P) = p$ and $a'_i b'_j \equiv a'_j b'_i \pmod{p}$, for all $i \neq j$.*

Under the above assumptions, if $\alpha = PQ = a_0 + a_1i + a_2j + a_3k$, and $P = b_0 + b_1i + b_2j + b_3k$ is a fixed point of $\tau_{Q,p}$, then $\alpha = PQ = Q'P$, for some $Q' \in \mathcal{H}$. We have the system of congruences

$$\left\{ \begin{array}{l} a_0 b_1 \equiv a_1 b_0 \\ a_0 b_2 \equiv a_2 b_0 \\ a_0 b_3 \equiv a_3 b_0 \\ a_1 b_2 \equiv a_2 b_1 \\ a_1 b_3 \equiv a_3 b_1 \\ a_2 b_3 \equiv a_3 b_2 \end{array} \right. \pmod{p} \quad (3.2)$$

The first three congruences can be condensed into the unique congruence

$$a_0 \mathcal{V}(P) \equiv b_0 \mathcal{V}(\alpha) \pmod{p},$$

and the last three congruences are simply,

$$\mathcal{V}(\alpha) \times \mathcal{V}(P) \equiv 0 \pmod{p}.$$

We have that $p \nmid a_0 b_0$, because if $p \mid a_0 b_0$, since $N(P) = p$, p cannot divide b_0 , thus p must divide a_0 . However, $a_0 = P \cdot \bar{Q}$, thus we would have that $p \mid Q$, which cannot happen. Therefore, the first congruence implies the second one. So, modulo p , the vector parts of α and P are colinear.

We know that from the Remark 1.5 that two quaternions commute if and only if their vector parts are colinear, and so, modulo p , we must have:

$$\begin{aligned} \alpha P - P\alpha &= 0 \\ \Leftrightarrow (PQ)P - P(PQ) &= 0 \\ \Leftrightarrow P(QP - PQ) &= 0 \\ \Leftrightarrow P(2\mathcal{V}(Q) \times \mathcal{V}(P)) &= 0. \end{aligned}$$

With this in mind, imagine that we have a rational odd prime p , and $Q = a + bi + cj + dk \in \mathcal{H}$ such that $(b, c, d) \neq (0, 0, 0)$ modulo p , $N(Q) = q$, and $\left(\frac{a^2 - q}{p}\right) = 0$, so there is only one fixed point. It is easy to know directly which Hurwitz prime P is fixed by $\tau_{Q,p}$ we only have check for the $p + 1$ primes, up to unit-migration, which one satisfies, modulo p :

$$P(\mathcal{V}(Q) \times \mathcal{V}(P)) = 0.$$

Now, if we have a Hurwitz Prime P with norm p , one can wonder which primes Q make it a fixed point of the metacommutation map $\tau_{Q,p}$. In particular, which primes Q make it the only fixed point of the map. To motivate this issue, we show an example.

Example 3.12. Let $P = 2 + i$, so $N(P) = 5$. We want to find $Q = a + bi + cj + dk$ with, $N(Q) = q$, that only fixes P . Thus, it must satisfy $(b, c, d) \neq (0, 0, 0)$ modulo p , and from Theorem 3.9 it must also satisfy

$$\left(\frac{a^2 - q}{5}\right) = 0 \Leftrightarrow a^2 \equiv q \Leftrightarrow b^2 + c^2 + d^2 \equiv 0 \pmod{5}.$$

If we compute $\mathcal{V}(Q) \times \mathcal{V}(P)$, we get the quaternion $D = dj - ck$. Then, we must have,

$$PD \equiv 0 \pmod{5},$$

which means that,

$$(2d + c)j + (d - 2c)k \equiv 0 \pmod{5},$$

and so we derive the following system

$$\begin{cases} 2d = -c \\ d = 2c \end{cases} \pmod{5}.$$

which is equivalent to $3d = c \pmod{5}$. Therefore, we are looking for a prime Q such that

$$\begin{cases} b^2 + c^2 + d^2 = 0 \\ 3d = c \end{cases} \pmod{5}.$$

If we let $b = 0$, then, modulo 5,

$$b^2 + c^2 + d^2 = (3d)^2 + d^2 = 0,$$

so we only need to find a such that q is prime. For example, if $d = 3$, then from $3d = c$, follows $c = 4$, so we need to find a , such that $a^2 + 4^2 + 3^2 = a^2 + 25$ is prime. If we take, for example, $a = 2$, it is done, and our quaternion is $Q = 2 + 4j + 3k$. Indeed, if $p = 5$ and $Q = 2 + 4j + 3k$, the metacommutation map $\tau_{Q,p}$ fixes only $P = 2 + i$. More generally, if $b = 0$ and we choose a number d , we only need to find a c such that $3d \equiv c \pmod{5}$ and a such that $a^2 + d^2 + c^2$ is prime.

The above calculation seems a bit cumbersome, especially when we consider rational primes p bigger than 5. Therefore, we look at this problem in another angle. If we recall Proposition 1.4, we can write the first congruence of 3.2 as,

$$\begin{aligned} (P \cdot \bar{Q})b_1 - b_0(P \cdot i\bar{Q}) &= 0 \\ P \cdot (b_1 - b_0i)\bar{Q} &= 0 \Leftrightarrow \Re((b_1 + b_0i)PQ) \equiv 0 \pmod{p}. \end{aligned}$$

Similarly, we also have for the other two congruences that,

$$\begin{aligned} P \cdot (b_2 - b_0j)\bar{Q} &= 0 \Leftrightarrow \Re((b_1 + b_0j)PQ) \equiv 0 \pmod{p}, \\ P \cdot (b_3 - b_0k)\bar{Q} &= 0 \Leftrightarrow \Re((b_1 + b_0k)PQ) \equiv 0 \pmod{p}. \end{aligned}$$

In our case, the last three equations of 3.2 are implied by the first three, thus, from the above calculations, we have:

Proposition 3.13. *Given a Hurwitz prime $P = b_0 + b_1i + b_2j + b_3k$ of odd norm p , and a prime quaternion Q such that $N(Q) = q$, then P is a fixed point of $\tau_{Q,p}$ if and only if $\Re(D_iPQ) = 0 \pmod{p}$, where $D_1 = b_1 + b_0i$, $D_2 = b_2 + b_0j$, and $D_3 = b_3 + b_0k$.*

However, the last three congruences also imply,

$$\begin{aligned} P \cdot [(b_1 - b_0i)\bar{Q} + (b_2 - b_0j)\bar{Q} + (b_3 - b_0k)\bar{Q}] &\equiv 0 \pmod{p} \\ P \cdot [(b_1 + b_2 + b_3 - b_0(i + j + k))\bar{Q}] &\equiv 0 \pmod{p}, \end{aligned}$$

which is equivalent to:

$$[(b_1 + b_2 + b_3 + b_0(i + j + k))Q]P \cdot 1 \equiv 0 \pmod{p}.$$

Corollary 3.14. *Given a Hurwitz prime $P = b_0 + b_1i + b_2j + b_3k$ of norm p , and a prime quaternion Q such that $N(Q) = q$, then P is a fixed point of $\tau_{Q,p}$ if $\Re(DPQ) = 0 \pmod{p}$, where $D = (b_1 + b_2 + b_3) + b_0i + b_0j + b_0k$.*

If we know that for a given Q , $\left(\frac{a^2 - q}{p}\right) = 0$, and we want to see if a given P is a fixed point (in fact, the only fixed point), we can first see $\Re(DPQ) = 0$. However, one should note that this is not an equivalence. Imagine that our P is again $2 + i$, and we want to find a Q such that P is the only fixed point of $\tau_{Q,p}$, then with the help of SageMath, we can produce the following code, for example, for the first 50 primes.

```

1 Gp()
2 from math import *
3 Primos=gp.Prime(50)
4
5 def PossiQ(p):
6     a=[]
7     am=[]
8     Q=[]
9     x=0
10    for i in range(1,int((p+1)/2)):
11        a.append(i**2)
12    for i in range(int((p-1)/2)):
13        for q in range(50):
14            if (a[i] < Primes[q]) and (a[i])%p==Primes[q]%p:
15                Q.append(Primes[q])
16    return(Q)
17
18 def FixedbyQ(P):
19     p=gp.qnorm(P)
20     L=PossiQ(p)
21     L.sort()
22     x=[]
23     V=[]
24     for i in range(len(L)):
25         V=gp.PrimosT(L[i])
26         for j in range(1,len(V)+1):
27             B=gp.AllLassoc(gp.quat(V[j][1],V[j][2],V[j][3],V[j][4]))
28             for k in range(1, len(B)+1):
29                 C=list(B[k])
30                 J=gp.quat(C[0],C[1],C[2],C[3])
31                 if (C[0]**2)%p==gp.qnorm(J)%p and (C[1]%7,C[2]%7,C[3]%7) !=(0,0,0):
32                     D=gp.quat(P[1,2]+P[1,3]+P[1,4],P[1,1],P[1,1],P[1,1])
33                     R=D*P*J
34                     if R[1,1]%p==0%p:
35                         D1=gp.quat(P[1,2],P[1,1],0,0)
36                         D2=gp.quat(P[1,2],0,P[1,1],0)
37                         D3=gp.quat(P[1,2],0,0,P[1,1])
38                         R1=D1*P*J
39                         R2=D2*P*J
40                         R3=D3*P*J
41                         if R1[1,1]%p==0%p and R2[1,1]%p==0%p and R3[1,1]%p==0%p:
42                             x.append(C)
43     x.sort()
44     return x

```

Remark 3.15. The functions **qnorm**, **AllLassoc** and **quat** are defined in appendix B.

The result is a list of quaternions, in which appears, as previously calculated, the quaternion $2 + 4j + 3k$. One should also note that, as we already seen in Remark 2.3, if a quaternion Q fixes the given P , then $\bar{Q}$ also fixes it. So, half the results we obtain are essentially the same.

Appendix A

Semisimplicity

In Chapter 2 we mentioned the concept of semisimplicity without details. The purpose of this appendix is to make everything clear. We follow [Lam91].

Definition A.1. Let R be a ring, and M be a (left) R -module.

1. M is called a **simple** (or irreducible) R -module if $M \neq 0$, and M has no R -submodules other than (0) and M .
2. M is called a **semisimple** (or completely reducible) R -module if every R -submodule of M is an R -module direct summand of M .

Note that, according to these definitions, the zero module is semisimple, but not simple. Also if we work in the category of commutative rings, simple commutative rings are precisely fields.

For any minimal left ideal I in a ring R , let S_I be the sum of all the minimal left ideals of R which are isomorphic to S_I as left R -modules.

Lemma A.2. *The following general properties of S_I are valid without any assumptions on the ring R .*

1. S_I is an ideal of R .
2. If I, I' are minimal left ideals which are not isomorphic as left R -modules, then $S_I \cdot S_{I'} = 0$.

Proof. For 1, it is enough to show that, if B is a minimal left ideal with $B \cong I$ (as left R -modules), then $B \cdot r \subseteq S_I$ for any $r \in R$. But $B \cdot r$ (as a left R -module) is a homomorphic image of B , so we can only have $B \cdot r = 0$ or $B \cdot r \cong B \cong I$. In either case, $B \cdot r \subseteq S_I$. For 2, it is enough to show that $I \cdot I' = 0$. Assume, on the contrary, that $I \cdot x' \neq 0$ for some $x' \in I'$. Since I' is a minimal left ideal, we must have $I \cdot x' = I'$. But then $I \cong I \cdot x' = I'$ (as left R -modules), a contradiction. □

If we work in the category of commutative rings, then the decomposition argument in the proof of the previous lemma shows that any semisimple commutative ring is a finite direct product of fields (and conversely). A square matrix or, in other words, a linear operator T on

a finite-dimensional vector space V over a field k is said to be **semisimple** if and only if any T -invariant subspace of V has a T -invariant complement. It can be seen that T is semisimple if and only if the subalgebra $k[T]$ of $\text{End}_k(V)$ is semisimple. Now, if $m(x)$ is the minimal polynomial of T , and

$$m(x) = m_1(x)^{e_1} \cdots m_r(x)^{e_r} \in k[x],$$

where the $m_i(x)$'s are its distinct irreducible factors, then

$$k[T] \cong \frac{k[x]}{(m(x))} \cong \prod_{i=1}^r \frac{k[x]}{(m_i(x)^{e_i})}.$$

This gives a decomposition of $k[T]$ into a finite direct sum of indecomposable ideals. It follows that $k[T]$ is semisimple if and only if each

$$k[x]/(m_i(x)^{e_i})$$

is a field, i.e., if and only if each $e_i = 1$. Therefore, a linear operator T of V is semisimple if and only if the minimal polynomial of T is square free. Note that, in the special case when k is algebraically closed, this is simply saying that T is semisimple if and only if it is diagonalizable. It also follows that an operator is semisimple if and only if it is diagonalizable over the algebraic closure of k . To see this, let A be the square matrix associated with T . Then notice that the minimal polynomial m of A will remain the same when extending the base field k to its algebraic closure $\bar{k}$. Since A is diagonalizable over $\bar{k}$, m splits into distinct linear factors over $\bar{k}$, and this is equivalent to saying that m decomposes into distinct irreducible factors over k .

Appendix B

SageMath auxiliar code

Useful functions used in Chapter 3.

```
1 Gp()
2
3 quat(a,b,c,d)=[a,b,c,d;-b,a,-d,c;-c,d,a,-b;-d,-c,b,a];
4
5 qconj(a)=quat(a[1,1],-a[1,2],-a[1,3],-a[1,4]);
6
7 qvec(a)=[a[1,2];a[1,3];a[1,4]];
8
9 qnorm(a)=(a*qconj(a))[1,1];
10
11
12 unid=[quat(1,0,0,0),quat(-1,0,0,0),quat(0,1,0,0),quat(0,-1,0,0),quat(0,0,1,0),
      quat(0,0,-1,0),quat(0,0,0,1),quat(0,0,0,-1),quat(1/2,1/2,1/2,1/2),quat
      (-1/2,-1/2,-1/2,-1/2),quat(1/2,1/2,1/2,-1/2),quat(-1/2,-1/2,-1/2,1/2),quat
      (1/2,1/2,-1/2,1/2),quat(-1/2,-1/2,1/2,-1/2),quat(1/2,-1/2,1/2,1/2),quat
      (-1/2,1/2,-1/2,-1/2),quat(1/2,1/2,-1/2,-1/2),quat(-1/2,-1/2,1/2,1/2),quat
      (1/2,-1/2,1/2,-1/2),quat(-1/2,1/2,-1/2,1/2),quat(1/2,-1/2,-1/2,1/2),quat
      (-1/2,1/2,1/2,-1/2),quat(1/2,-1/2,-1/2,-1/2),quat(-1/2,1/2,1/2,1/2)];
13
14 AllLassoc(q)={
15     local(lt);
16     lt=listcreate(24);
17     for(i=1,24,listput(lt,quatb(unid[i]*q)));
18     return(lt);
19 }
```


Bibliography

- [AADGS13] M. Abouzaid, J. Alper, S. DiMauro, J. Grosslight, and D. Smith. “Common left- and right-hand divisors of a quaternion integer”. In: *Journal of Pure and Applied Algebra* 217 (2013), pp. 779–785.
- [CK15] H. Cohn and A. Kumar. “Metacommutation of Hurwitz Primes”. In: *Proceedings of the American Mathematical Society* 143 (2015), pp. 1459–1469.
- [CP12] B. Coan and C. Perng. “Factorization of Hurwitz Quaternions”. In: *International Mathematical Forum* 7 (2012), pp. 2143–2156.
- [CS03] J. H. Conway and D. A. Smith. *On Quaternions and Octonions: their Geometry, Arithmetic, and Symmetry*. Natick: A K Peters, Ltd., 2003.
- [FGS15] A. Forsyth, J. Gurev, and S. Shrima. “Metacommutation Action as a Group Action on the Projective Line over $\mathbb{F}_p$ ”. In: *Proceedings of the American Mathematical Society* 143 (2015), pp. 1459–1469.
- [IR90] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*. Springer, 1990.
- [Lam05] T. Y. Lam. *Introduction to Quadratic Forms over Finite Fields*. American Mathematical Society, 2005.
- [Lam91] T. Y. Lam. *A First Course in Noncommutative Rings*. Springer, 1991.
- [Lip86] M. Lipschitz. “Recherches sur la Transformation, par des Substitutions Réelles, d’une Somme de Deux ou de Trois Carrés en Elle-même”. In: *Journal de Mathématiques Pures et Appliquées* 2 (1886), pp. 373–439.
- [LN96] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, 1996.
- [Pal40] G. Pall. “On the Arithmetic of Quaternions.” In: *Transactions of the American Mathematical Society* 47 (1940), pp. 487–500.
- [Per11] C. Perng. “Factorization of Lipschitz Quaternions”. preprint. 2011.
- [Rei88] M. Reid. *Undergraduate Algebraic Geometry*. Cambridge University Press, 1988.
- [Ser73] J.-P. Serre. *A Course in Arithmetic*. Springer, 1973.
- [Shi10] G. Shimura. *Arithmetic of Quadratic Forms*. Springer, 2010.
- [Tso20] N. Tsopanidis. “The Hurwitz and Lipchitz Integers and Some Applications”. PhD thesis. Faculdade Ciências da Universidade do Porto, 2020.