Noncommutative Rings

Bernie Luan

July 2020

1 Introduction

Even though most rings we study in algebraic geometry are commutative, noncommutative rings is also an important category of rings. The main type of noncommutative rings that we will study in this essay is the quaternion ring. We will first develop the basic theory of quaternions, then prove some preliminary theorems that will facilitate our proof of the Lagrange's Theorem, and end with some generalizations of the Lagrange's Theorem. The only necessary background expected would be experience with commutative ring theory; nevertheless, previous exposure of elementary number theory and linear algebra will facilitate your understanding.

2 Quaternions

Quaternions were invented by Irish mathematician William Hamilton as an extension of complex numbers to spaces. In this section, we will present such connection and necessary results to prove the following theorem.

Theorem 2.1 (Lagrange's Four-Square Theorem)**.** *Every positive integer is the sum of at most four squares.*

Lemma 2.2. *Any prime p is the sum of at most four squares.*

We will now show the two statements are equivalent and we will prove the lemma later.

Proof. Let $x_i, y_i \in \mathbb{Z}$, note $(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = (x_1y_1 + x_2y_2 + x_3y_3 + x_4 + y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 + x_4y_3)^2 + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2$. Then the two statements are equivalent by the fundamental theorem of arithmetic. This identity we used here is called the Euler's Four-Square Identity, and this identity is a lot easier to comprehend once we develop the basic theories of quaternions. ■

Definition 2.3. A number α is called an quaternion if it is in the form $\alpha = a+bi+cj+dk$, where $a, b, c, d \in \mathbb{R}$ and i, j, and k are the fundamental quaternion units and a,b,c, and d are called coordinates of α.

Define $q = a + bi + cj + dk$, and $q' = a' + b'i + c'j + d'k$, then they are equivalent if and only $a = a'$, $b = b'$, $c = c'$, and $d = d'$. For every quaternion, a is called real or scalar part while $bi+cj+dk$ is called vector part. An quaternion with a zero vector part is called real or scalar quaternion, and one with zero real part is called an vector quaternion. Addition is defined similar to how it is defined for vectors:

$$\begin{aligned} q + q' &= (a + bi + cj + dk) + (a' + b'ic'j + d'k) \\ &= (a + a') + (b + b')i + (c + c')j + (d + d')k \end{aligned}$$

For an scalar $\lambda \in R$, the scalar multiplication $\lambda q = \lambda a + (\lambda b)i + (\lambda c)j + (\lambda d)k$. However, scalar multiplication is simply a special case of the Hamilton product.

Definition 2.4. For quaternions q and q', the Hamilton product $p * q = e + fi + gj + hk$, where

$$\begin{aligned} e &= aa' - bb' - cc' - dd' \\ f &= ab' + ba' + cd' - dc' \\ g &= ac' - bd' + ca' + db' \\ h &= ad' + bc' - cb' + da' \end{aligned}$$

In particular, $i^2 + j^2 + k^2 = -1$, $i = jk = -kj$, $j = ki = -ik$, and $k = ij = -ji$

Definition 2.5. The conjugate of q is denoted $\bar{q}$ and it is defined as the quaternion $\bar{q} = a - bi - cj - dk$ such that $q * \bar{q} = a^2 + b^2 + c^2 + d^2$. The value of $q * \bar{q}$ is also called the norm of q, denoted $||q||$.

For arbitrary quaternion p and q, $||p * q||=||p||||q||$. This can be shown through some simple but tedious calculations. Note this property of quaternions imply the Euler Four-Square Identity.

Definition 2.6. A quaternion with a norm of 1 is called an unit quaternion, and for a quaternion q, the unit quaternion $\frac{q}{||q||}$ is defined as the versor of q.

As we defined the operations of the quaternions, we can now determine the structure of quaternions.

Proposition 2.7. *The set of all quaternions is a noncommutative division ring with the operations being component addition and Hamilton product.*

Proof. Suppose we have $p = a + bi + cj + dk$, $p' = a' + b'i + c'j + d'k$, and $q = e + fi + gj + hk$. Then $p + q = (a + e) + (b + f)i + (c + g)j + (d + h)k = (e + a) + (f + b)i + (g + c)j + (h + d)k = q + p$. This prove commutativity under addition and now we will prove associativity.

$$\begin{aligned} (p + p') + q &= ((a + a') + e) + ((b + b') + f)i + ((c + c') + g)j + ((d + d') + h)k \\ &= (a + (a' + e)) + (b + (b' + f))i + (c + (c' + g))j + (d + (d' + h))k \\ &= p + (p' + q) \end{aligned}$$

The additive identity is simply the real quaternion 0 since $p + 0 = p$ for all quaternion p. And for every quaternion p, the additive inverse is simply $-p$ since $p + (-p) = (a + (-a)) + (b + (-b))i + (c + (-c))j + (d + (-d))k = 0$.

Associativity of multiplication and distributivity of multiplication is a rather easy but tedious calculation and it would be left to the reader to check that. Note the i component of $p*q$ is $af+be+ch-dg \neq eb+fa+gd-hc$, which is the i component of $q * p$. Thus, multiplication is noncommutative. Since $1 * p = p$ for every quaternion p, the multiplicative identity is simply the real quaternion 1.

Note $||p|| = ||\bar{p}||$, and $p * \bar{p} = ||p||$. Thus, $p * \frac{\bar{p}}{||\bar{p}||} = 1$, implying the multiplicative inverse for every nonzero quaternion p is the versor of the conjugate p. This implies that the ring of quaternions is a division ring, and it is denoted $\mathbb{H}$ in honor of Hamilton. ■

Now we know $\mathbb{H}$ is a noncommutative ring, it would be natural to ask when are the elements commutative. Therefore, we have the following definition.

Definition 2.8. The center of a ring R is a subring consists of all elements x such that $x * y = y * x$ for all $y \in R$, and it is denoted $Z(R)$.

Proposition 2.9. *$Z(\mathbb{H})$ is a field and it is the set of all real quaternions.*

Proof. If quaternion $p = a + bi + cj + dk \in Z(\mathbb{H})$, then it must satisfy the folowing system of identity by definition of the Hamilton product,

$$\begin{aligned} ae - bf - cg - dh &= ea - fb - gc - hd \\ af + be + ch - dg &= eb + fa + gd - hc \\ ag - bh + ce + df &= ec - fd + ga + hb \\ ah + bg - cf + de &= ed + fc - gb + ha \end{aligned}$$

Therefore,

$$\begin{aligned} ch - dg &= gd - hc \\ df - bh &= hb - fd \\ bg - cf &= fc - gb \end{aligned}$$

This is true if and only if $b = c = d = 0$, which implies p is a real quaternion. Conversely, let there be a $\lambda \in R$ and note $\lambda * p = \lambda a + (\lambda b)i + (\lambda c)j + (\lambda d)k = a\lambda + (b\lambda)i + (c\lambda)j + (d\lambda)k = p * \lambda$. Since every $\lambda \in R$ is a real quaternion, $Z(\mathbb{H})$ is equivalent to the set of all real quaternions and $Z(\mathbb{H}) = \mathbb{R}$. Since $\mathbb{R}$ is a field, so is $Z(\mathbb{H})$. ■

Throughout the section, we have seen many similarities between quaternions and complex numbers, and we will now establish another one.

Definition 2.10. A quaternion is called a Hurwitz integer or a integral quaternion and it is in the set $H = \{p = a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z} \quad \text{or} \quad a, b, c, d \in \mathbb{Z} + \frac{1}{2}\}$. If $a, b, c, d \in \mathbb{Z}$ only, then it is called a Lipschitz integer. A Hurwitz integer is odd or even based on whether its norm is odd or even.

The Hurwitz and Lipschitz integer is very similar to the Gaussian integer or $\mathbb{Z}[i]$, and we will only need a couple more defintions to prove the main theorem.

Definition 2.11. A quaternion q is called an unity if both q and q^{-1} are Hurwitz integers, and the norm of q is 1.

Note if a Hurwitz integer $p = a + bi + cj + dk$ is an unity, then there are two possibilities: 1. If $a, b, c, d \in \mathbb{Z}$, and $a^2 + b^2 + c^2 + d^2 = 1$, then only one of a^2, b^2, c^2, d^2 equals 1 and the rest are zero. 2. If $a, b, c, d \in \mathbb{Z} + \frac{1}{2}$, then $a^2 = b^2 = c^2 = d^2 = \frac{1}{4}$. Thus, there are only 24 possible unities, namely $\pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k)$, and every Hurwitz quaternion can be written in the form of $h = k_0\rho + k_1 i + k_2 j + k_3 k$, where $\rho = \frac{1}{2}(\pm 1 \pm i \pm j \pm k)$ and $k_0, k_1, k_2, k_3 \in \mathbb{Z}$.

Definition 2.12. If p is an arbitrary quaternion and q is an unity, then pq and qp are called associates of p.

Proposition 2.13. *The norm of the associates of p is the same as p, and the associates of a Hurwitz integer is also a Hurwitz integer.*

Proof. $||pq|| = ||p||||q|| = ||p||$, $||qp|| = ||q||||p|| = ||p||$. Since all unities are Hurwitz integers, and the product of two Hurwitz integers is also a Hurwitz integer, then all associates of a Hurwitz integer are also Hurwitz integers. ■

Definition 2.14. Let $p, q, r \in \mathbb{H}$, and $r = p * q$, then p is called the left-hand divisor of r and q is the right-hand divisor.

3 Lagrange's Theorem

With all basic definitions and propositions established, I will now present some prelimnary theorems which are necessary for the proof of the main theorem. Most of the material below are from Section 20.7 of the 6th edition of Hardy and Wright.

Theorem 3.1. *If h is an Hurwitz integer, then at least one of its associates has integral coordinates; if h is odd, then at least one of its associates has non-integral coordinates.*

Proof. If h has integral coordinates, then $1 * h$ also has integral coordinates. Now suppose h has no integral coordinates, then h can be written in the form $h = (a_0 + a_1 i + a_2 j + a_3 k) + \frac{1}{2}(\pm 1 \pm i \pm j \pm k) = a + b$, where a_0, a_1, a_2, a_3 are even. This implies any associates of a has integral coordinates. Note $\bar{b}$ is an unity, thus, $b * \bar{b} = 1$ is an associate of b. This implies $h * \bar{b}$ has integral coordinates.

If h does not have integral coordinates, h is odd since for odd integer a, b, c, d, $\frac{a^2+b^2+c^2+d^2}{4}$ is odd. Then $1 * h$ does not have integral coordinates. Now suppose h has integral coordinates, then it is in the form $h = (a_0 + a_1 i + a_2 j + a_3 k) + (b_0 + b_1 i + b_2 j + b_3 k)$ where a_0, a_1, a_2, a_3 are even integers and b_0, b_1, b_2, b_3 are

either 1 or 0. Note in order for h to be odd, then either one or three of them need to be one. So now we need to prove every element in the set S where $S = \{1, i, j, k, 1+i+j, 1+i+k, 1+j+k, i+j+k\}$ has an associate with non-integral coordinates. Note $1*\rho, i*\rho, j*\rho, k*\rho$ all have non-integral coordinates and

$$\begin{aligned} 1+i+j &= 1+i+j+k-k \\ 1+i+k &= 1+i+j+k-j \\ 1+j+k &= 1+i+j+k-i \\ i+j+k &= 1+i+j+k-1 \end{aligned}$$

Since all associates of $1+i+j+k$ have integral coordinates, every element in S has an associate with non-integral coordinates. Hence, h has an associate with non-integral coordinates. ■

Theorem 3.2. *If h is an Hurwitz integer, m an positive integer, then there exists a Hurwitz integer p such that* $||h - mp|| < m^2$.

Proof. The theorem is trivial when $m = 1$, so suppose $m > 1$, and let $h = a_0\rho + a_1 i + a_2 j + a_3 k, \quad p = b_0\rho + b_1 i + b_2 j + b_3 k$. Then the coordinates of $h - mp$ are $\frac{1}{2}(a_0 - mb_0), \frac{1}{2}(a_0 + 2a_1 - m(b_0 + 2b_1)), \frac{1}{2}(a_0 + 2a_2 - m(b_0 + 2b_2)), \frac{1}{2}(a_0 + 2a_3 - m(b_0 + 2b_3))$. Now we can choose appropriate b_0, b_1, b_2, b_3 such that the following hold:

$$\begin{aligned} |\frac{1}{2}(a_0 - mb_0)| &< \frac{1}{4}m \\ |\frac{1}{2}(a_0 + 2a_1 - m(b_0 + 2b_1))| &< \frac{1}{2}m \\ |\frac{1}{2}(a_0 + 2a_2 - m(b_0 + 2b_2))| &< \frac{1}{2}m \\ |\frac{1}{2}(a_0 + 2a_3 - m(b_0 + 2b_3))| &< \frac{1}{2}m \end{aligned}$$

Implying, $||h - mp|| \leq \frac{1}{16}m^2 + \frac{3}{4}m^2 < m^2$. ■

Theorem 3.3. *If h and t are Hurwitz integers, and* $p \neq 0$*, then there exists Hurwitz integer q and r such that* $h = t * q + r$ *where* $||r|| < ||q||$.

Proof. Let $\kappa = h * \bar{t}$, $m = t * \bar{t}$, and p be the same as in the previous theorem, and note $(h - qt) * \bar{t} = \kappa - mp$. Then $||h - qt||||\bar{t}|| < m^2$ by the previous theorem. In addition, $||r|| = ||(h - qt)|| < m = ||t||$ ■

Definition 3.4. Two Hurwitz integer h and p have a highest common right-hand divisor δ if the following holds: 1. δ is a right hand divisor of h and p. 2. Every right hand divisor of h and p is also a right hand divisor of δ.

Definition 3.5. If S is a set of Hurwitz integers that is not (0), then it is a right ideal if it satisfies the following properties: 1. For $\alpha, \beta \in S$, $\alpha \pm \beta \in S$. 2. For $\alpha \in S$, $h\alpha \in S$ for every Hurwitz integer h. Note this is different from a normal ideal since $h\alpha \neq \alpha h$

Theorem 3.6. *For every right ideal $S \in H$, S is a principal right ideal.*

Proof. Note if S is a principal right ideal (δ) where δ is a Hurwitz integer, and $r \in S$, $||r|| < ||\delta||$ implies $r = 0$. Now if $a \in S$, then $a - q\delta \in S$. By previous theorem, we can choose q such that $||r|| = ||a - q\delta|| < ||\delta||$. Thus, $r = 0$ and $a = q\delta$, implying S is a principal right ideal. ■

Theorem 3.7. *Any two Hurwitz integer a and b, which one of them is nonzero, have a highest common right hand divisor, that is unique except for a left-hand unit factor, is in the form $\delta = ma + kb$, where $m, k \in H$.*

Proof. Let $S = \{ma+kb\}$, S is then a right ideal and also a principal right ideal by the previous theorem. Thus, for every element $ma + kb \in S$, $ma + kb = \lambda\delta$ for some integer λ. In particular, there are m and k such that $ma + kb = \delta$. Since $a, b \in S$, δ is a common right hand divisor of a and b, and every common right hand divisor is also a right hand divisor of every element in S, implying that they are also right hand divisor of δ. Thus, δ is the highest common right hand divisor of a and b.

If there are two highest common right hand divisor δ, δ', let $\delta' = \lambda\delta$, $\delta = \lambda'\delta'$ for integral λ, λ', then $\delta = \lambda\lambda'\delta$, and λ is a unity. If δ is a unity, then there are m,k such that $ma + kb = 1$, which we denote $(a, b)_r = 1$ ■

Remark 3.8. The two previous theorems and the definition also apply to left hand ideal, but we do not have enough space to prove them here.

Theorem 3.9. *If a in a Hurwitz integer and $b > 0$ is a real quaternion with integer coordinates, then a necessary and sufficient condition that $(a, b)_r = 1$ is $(||a||, ||b||) = 1$.*

Proof. If $(a, b)_r = 1$, then there are Hurwitz integer m, k such that $ma+kb = 1$. Then $||ma|| = ||1 - kb|| = (1 - kb)(1 - \bar{k}b) = 1 - kb - \bar{k}b + b^2||k||$. Then $(||a||, ||b||) = 1$. ■

Definition 3.10. A Hurwitz integer π whose norm is not 1 is prime if its only divisors are its associates and unities.

Theorem 3.11. *An Hurwitz integer π is prime if and only if its norm is a prime number.*

Lemma 3.12. *A prime number p is not a prime quaternion.*

Remark 3.13. We will combine the proof of the two theorem by proving the lemma first and show the theorem is a simple corollary of the lemma. However, we need to assume a number theoretic theorem, and the proof of the theorem can be found in section 6.7 of Hardy and Wright.

Theorem 3.14. *If p is an odd prime, then there are numbers x and y such that $1 + x^2 + y^2 = mp$, where $0 < m < p$.*

Proof. If the norm of π is a prime number, and $\pi = ab$, then either the norm of a or the norm of b is 1, so one of them is unity and π is prime.

To prove the converse, we will first prove the lemma. Since $2 = (1+i)(1-i)$, we can restrict our attention to odd primes. By previous theorem, there are integers r and s such that $0 < r < p$, $0 < s < p$, such that $1 + r^2 + s^2 \equiv 0 (\text{mod p})$. If $a = 1 - sj - rk$, the norm of a is $1 + r^2 + s^2$ which is congruent to 0 mod p, and $(||a||, p) > 1$. Then by Theorem 3.9, a and p have a common right hand divisor δ that is not unity such that $a = a_1\delta, p = p_1\delta$. If p_1 is a unity, then δ is an associate of p. In addition, p divides all coordinates of $a = a_1 p_1^{-1} p$, especially 1, which is impossible, and this proves the lemma.

Now we prove the theorem, Let π be a prime quaternion and p a prime divisor of the norm of π. By Theorem 3.9, π and p have a common right hand divisor π' that is not a unity. Since π is prime, π' is an associate of π. Since $p = \lambda\pi'$, where $\lambda \in H$, and note $p^2 = ||\lambda||||\pi'|| = ||\lambda||||\pi||$, so the norm of λ is either 1 or p. If it is p, then p would be an associate of π, which is false by lemma. Hence the norm of π is p, and that completes the proof. ■

Now we are ready to prove the Lagrange's theorem.

Proof. If p is a prime number, $p = \lambda\pi$, where $||\lambda|| = ||\pi|| = p$, If π has integral coordinates, let $\pi = a + bi + cj + dk$, $p = ||\pi|| = a^2 + b^2 + c^2 + d^2$. If π does not have integer coordinates, then there is a associate of π that has integer coordinates by Theorem 3.1, and $p = ||\pi|| = ||\pi'||$, and this proves the lemma which proves the Lagrange's Theorem. ■

Corollary 3.15. *If p is an odd prime number, then 4p is the sum of the square of four odd integers.*

Proof. If p is odd, we can select an associate of $\pi = a_0 + a_1 i + a_2 j + a_3 k$ that has coordinates that are halves of odd integers by Theorem 3.1. Thus,

$$p = ||\pi|| = ||\pi'|| = (a_0 + \frac{1}{2})^2 + (a_1 + \frac{1}{2})^2 + (a_2 + \frac{1}{2})^2 + (a_3 + \frac{1}{2})^2$$

.

$$4p = (2a_0 + 1)^2 + (2a_1 + 1)^2 + (2a_2 + 1)^2 + (2a_3 + 1)^2$$

■

4 Generalizations of Lagrange's Theorem

Theorem 4.1 (Fermat-Cauchy Polygonal Number Theorem)**.** *Every positive integer is the sum of at most n n-gonal numbers.*

Remark 4.2. The triangular number case was proved by Gauss as he wrote in his diary "EYPHKA!, num=$\triangle + \triangle + \triangle$". The general case was eventually proved by Cauchy.

Theorem 4.3 (Hilbert-Waring Theorem)**.** *For every positive integer k there exists an positive integer s such that every positive integer can be represented as a sum of s natural number to the kth power.*

Remark 4.4. The proof of the theorem above will not be presented here. There are mainly two way of proving this, first by Hilbert that does not present a way of finding s, the other by Hardy and Littlewood which presents a analytic way of finding s for certain values. The proof by Hilbert relies on a powerful polynomial identity and a 25-fold integral and is a technical tour de force(A simpler version of his proof can be found at The American Mathematical Monthly Vol.78, No.1 (Jan. 1971), pp.10-36); however, we still can not manipulate s except for a certain number of k. The minimum of s is usually denoted $g(k)$ and $G(k)$ is the least s such that every integer greater than some integer M can be represented as a sum of $G(k)$ integer to the kth power. A systematic way of finding both values for every k is still a major unsolved problem in mathematics.