Chapter 7. Selected Topics

Section 7.4. Integral Quaternions and the Four-Square Theorem

Note. In Elementary Number Theory (MATH 3120), we proved that every positive integer can be written as the sum of four squares of integers. See Lagrange's Four-Square Theorem (Theorem 19.1) in my online notes on Section 19. Sums of Four Squares. The result is called "Lagrange's Four-Square Theorem" because it was proved by Joseph Louis Lagrange in 1770. Historical details can be found in the number theory notes just mentioned. In this section, we introduce the noncommutative division ring of real quaternions and use it to give a proof of Lagrange's result. We'll consider a subring H of the quaternions (a ring similar to the Guassian integers from $\mathbb{C}$, but based on "integral quaternions") and classify the left ideals of H (in Lemma 7.4.6). This will lead to our proof of Lagrange's Four-Square Theorem.

Note. We denote the noncommutative division ring of real quaternions as Q (also often denoted $\mathbb{H}$ in commemoration Sir William Rowan Hamilton who introduced them in 1843). A formal definition of the quaternions is given in Modern Algebra 2 (MATH 5420) in Section III.1. Rings and Homomorphism and in Quaternions—An Algebraic View (Supplement).

Definition. For $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ in Q, the *adjoint* (or *conjugate*) of x, denoted x^*, is defined as $x^* = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$.

Lemma 7.4.1. The adjoint in Q satisfies:

1. $x^{**} = x$,

2. $(\delta x + \gamma y)^* = \delta x^* + \gamma y^*$, and

3. $(xy)^* = y^* x^*$

for all $x, y \in Q$ and for all real δ and γ.

Definition. If $x \in Q$ then the *norm* of x, denoted $N(x)$, is defined as $N(x) = xx^*$.

Note. We might be interested more in the "modulus" of $x \in Q$ which we should define as $|x| = \sqrt{xx^*}$. However, this idea of a norm N is common in the number theory setting. For example, in the Gaussian integers $\{a + bi \mid a, b \in \mathbb{Z}\}$ the norm is defined as $N(a + bi) = a^2 + b^2 = |a + bi|^2$. See my online notes for Mathematical Reasoning (MATH 3000) on Section 7.2. The Gaussian Integers.

Lemma 7.4.2. For all $x, y \in Q$ we have $N(xy) = N(x)N(y)$.

Note. The next result is just a restatement of Lemma 7.4.2, but in terms of the "parts" of quaternions $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ and $y = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k$.

Lemma 7.4.3. Lagrange Identity.

If $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ and $\beta_0, \beta_1, \beta_2, \beta_3$ are real numbers then

$$(\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2)(\beta_0^2 + \beta_1^2 + \beta_2^2 + \beta_3^2) = (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3)^2$$
$$+(\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2)^2 + (\alpha_0\beta_2 - \alpha_1\beta_3 + \alpha_2\beta_0 + \alpha_3\beta_1)^2$$
$$+(\alpha_0\beta_3 + \alpha_1\beta_2 - \alpha_2\beta_1 + \alpha_3\beta_0)^2.$$

Note. The Lagrange Identity (Lemma 7.4.3) expresses the sum of four squares times the sum of another four squares equals the sum (in a specific way) of a sum of four squares. The identity is given in Note 19.A of my online Elementary Number Theory (MATH 3120) notes on Section 19. Sums of Four Squares. Similar to the Gaussian integers which are a subring of the complex numbers, we have the following subring of the quaternions.

Definition. The *Hurwitz ring* is the ring of integral quaternions:

$$H = \{m_0\zeta + m_1 i + m_2 j + m_3 k \mid m_0, m_1, m_2, m_3 \in \mathbb{Z}\},$$

where $\zeta = \frac{1}{2}(1 + i + j + k)$.

Note. Notice that the norm of ζ is 1, $N(\zeta) = \zeta\zeta^* = \frac{1}{4}(1^2 + 1^2 + 1^2 + 1^2) = 1$. In fact, every element of the Hurwitz ring is of norm a positive integer, as we claim next (along with the fact that H actually is a ring). That's why we refer to the "integral quaternions." We leave the proof of the next result "to the reader" (it is straightforward).

Lemma 7.4.4. *H is a subring of Q. If $x \in H$ then $x^* \in H$ and $N(x)$ is a positive integer for every nonzero $x \in H$.*

Note. It might seem odd (it does to me!) to consider the Hurwitz ring as the subring of Q instead of simply the ring

$$Q_0 = \{m_0 + m_1 i + m_2 j + m_3 k \mid m_0, m_1, m_2, m_3 \in \mathbb{Z}\}.$$

The reason we consider the larger ring H is because it has the properties we need to characterize its left-ideals. This is needed in our proof of Lagrange's Four-Square Theorem. Before classifying the left-ideals, we need a lemma.

Lemma 7.4.5. Left-Division Algorithm.
Let $a, b \in H$ with $b \neq 0$. Then there exists two elements $c, d \in H$ such that $a = cb + d$ and $N(d) < N(b)$.

Note. Recall from Introduction to Modern Algebra 2 (MATH 4137/5137) (see my online notes on Section V.26. Homomorphisms and Factor Rings; notice Definition 26.10) that:

> **Definition.** An additive subgroup N of a ring R satisfying the property $aN \subseteq N$ for all $a \in R$ is a *left-ideal*. An additive subgroup N of a ring R satisfying the property $Nb \subseteq N$ for all $b \in R$ is a *right-ideal*. An additive subgroup N of a ring R tht is both a left-ideal and a right-ideal is an *ideal*.

Now for the classification of left-ideals of H.

Lemma 7.4.6. Let L be a left-ideal of H. Then there exists an element $u \in L$ such that every element in L is a left-multiple of u; in other words, there exists $u \in L$ such that every $x \in L$ is of the form $x = ru$ where $r \in H$.

Note. We need one more lemma.

Lemma 7.4.7. If $a \in H$ then $a^{-1} \in H$ if and only if $N(a) = 1$.

Note. We will also need the well-known Wedderburn's Theorem, which states that every finite division ring is a field. This is stated in Introduction to Modern Algebra (MATH 4127/5127); see Theorem 24.10 of Section 24 "Noncommutative Examples" in John Fraleigh's *A First Course In Abstract Algebra*, 7th Edition, Addison Wesley (2003). It is proved (twice) in Isreal Herstein's *Topics in Algebra*, 2nd Edition, John Wiley & Sons (1975) in Section 7.2 "Wedderburn's Theorem on Finite Division Rings" as Theorem 7.2.1. It is (potentially) proved in Modern Algebra (MATH 5410/5420); see Thomas W. Hungerford' *Algebra*, Springer-Verlag (1974) in Section IX.6 "Division Algebras" as Corollary IX.6.9 (and a different proof based on cyclotomic polynomials it to be given in Exercise V.8.10).

Note. In Thomas W. Hungerford' *Algebra*, Springer-Verlag (1974) in Section III.2 "Ideals," we have the following as Exercise III.2.5:

> **Lemma 7.4.A.** A ring R with identity is a division ring if and only if R had no proper, nontrivial left ideals.

The "only if" part of this claim appears Isreal Herstein's *Topics in Algebra*, 2nd Edition, John Wiley & Sons (1975) in in Section 3.5 "More Ideals and Quotient Rings" as Exercise 3.5.1.

Note 7.4.A. We need one final claim before presenting Lagrange's Four-Square Theorem. We claim that in the Hurwitz ring H,

$$V = \{x_0\zeta + x_1 i + x_2 j + x_2 k \mid p \text{ divides all of } x_0, x_1, x_2, x_3\}$$

is a two-sided ideal and that the quotient ring H/V is isomorphic to

$$W_p = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \mid \alpha_0, \alpha_1, \alpha_3, \alpha_3 \in \mathbb{Z}_p\}.$$

We leave this as an exercise. Now we are ready to state and prove our main result.

Theorem 7.4.1. Lagrange's Four-Square Theorem.
Every positive integer can be expressed as the sum of squares of four integers.

Note. A generalization of the Four-Square Theorem was introduced by British mathematician Edward Waring (circa 1736–August 15, 1798) in 1770. *Waring's problem* asks whether each $k \in \mathbb{N}$ has an associated positive integer s such that every natural number is the sum of at most s natural numbers raised to the power k. The answer for $k = 2$ is "yes" and we see that $s \geq 4$ in this case. In fact the answer is "yes" for all $k \in \mathbb{N}$, as shown by David Hilbert in "Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem)," *Mathematische Annalen* **67**(3), 281–300 (1909). A copy can be viewed online on the

Springer webpage (accessed 4/19/2022). For $k \in \mathbb{N}$, define $g(k)$ as the minimum value of s which guarantees that every natural number is the some of s natural numbers raised to the power k. The Four-Square Theorem shows that $g(2) = 4$. Other known values of g are: $g(1) = 1$ (trivially), $g(3) = 9$, $g(4) = 19$, $g(5) = 37$, and $g(6) = 73$ (according to the Wikipedia page on Waring's Problem (accessed 4/19/2022). Additional historical details are in my online notes for Elementary Number Theory (MATH 3120) on Section 18. Sums of Two Squares.

Revised: 4/25/2022