$R_+(S)$ for Algebraic Numbers

Eddie Hu
under the direction of
Daniil Kalinov
Dr. Tanya Khovanova
Department of Mathematics
Massachusetts Institute of Technology

Research Science Institute
July 30, 2019

Abstract

In this paper, we try to calculate $R_+(S)$ for algebraic numbers S in order to show the existence of symmetric monoidal functors between Deligne categories $\mathrm{Rep}(S_t) \to \mathrm{Rep}(S'_t)$. We first evaluate $R_+(S)$ for rational S ($R_+(S) = \mathbb{Z}[\frac{1}{n}] = \mathbb{Z}[\frac{m}{n}]$). In the case where $S = \sqrt{n}$, we use the gained intuition from the rational case as well as quadratic reciprocity to reach certain conclusions about the possibilities of $R_+(S)$. We not only get $\mathbb{Z}[\sqrt{n}] \subset R_+(\sqrt{n})$, but also the stronger statement for $n = 2$ that $R_+(\sqrt{2}) = \mathbb{Z}[\frac{1}{p_1}, \frac{1}{p_2}, \ldots, \frac{1}{p_i}, \ldots][\sqrt{2}]$ for primes p_i such that $\left(\dfrac{2}{p_i}\right) \neq 1$.

Summary

Representation theory is a branch of mathematics that studies algebraic structures by representing their elements as vector spaces and linear transformations of these vector spaces. It allows one to utilize linear algebra techniques to simplify problems in abstract algebra. In this paper, we evaluate the properties of a specific algebraic structure $R_+(S)$ which is generated from a set of binomial coefficients of an algebraic number S. In order to further study this specific structure, we use number theoretical techniques to evaluate $R_+(S)$ for rational S and for $S = \sqrt{2}$.

1 Introduction

Representation theory as a field has been around since Gauss in the beginning of the 19th century, but was formally created by Frobenius about 100 years ago when he investigated characters of finite nonabelian groups. [1]

Representation theory allows one to study specific algebraic structures by representing their elements as vector spaces and linear transformations. Combining the fields of abstract algebra and linear algebra makes it possible to investigate many properties of algebraic structures.

Specifically, consider the Deligne category $\mathrm{Rep}(S_t)$, for $t \in \mathbb{C}$. One can think about it as a kind of algebraic continuation of the regular tensor categories of representations of S_n – $\mathbf{Rep}(S_n)$ for integer n. One interesting question about such categories is whether there is a symmetric monoidal functor between $\mathrm{Rep}(S_t)$ and $\mathrm{Rep}(S_{t'})$ for $t, t' \in \mathbb{C}$. The existence of such functors is dictated by the following lemma:

Lemma 1.1. *Symmetric monoidal functors between Deligne categories Rep*$(S_t) \to$ *Rep*$(S_{t'})$ *with* $t, t' \notin \mathbb{Z}_{\geq 0}$ *exist iff* $t \in R_+(t')$.

Here, $R_+(t')$ is the set of positive linear combinations of $\binom{t'}{k}$ (see definition 2.1 below). One important consequence of this result used below is that $R_+(t)$ is closed under composition. This means that if $t_1 \in R_+(t_2)$ and $t_2 \in R_+(t_3)$, when $t_1 \in R_+(t_3)$ and so $R_+(t_2) \subset R_+(t_3)$ (indeed, take a composition of functors).

Hence, in order to study functors between Deligne categories, we need to calculate $R_+(t)$ for different values of t. This is done in the current paper for rational t and for some algebraic t satisfying quadratic equations.

For a more detailed discussion of the above see [2].

2 Methods

For $x, k \in \mathbb{N}$, the binomial coefficient $\binom{x}{k}$ is the number of ways to choose k objects from x total ones such that order does not matter. We can calculate it for $x \geq k$ using the formula $\binom{x}{k} = \frac{x!}{k!(x-k)!}$.

This fact only works for non-negative integer values of x and k. However, we can generalize the definition of binomial coefficients to work for non-integer values of x. For $x \in \mathbb{C}$ and $k \in \mathbb{N}$, $\binom{x}{k} = \frac{x(x-1)(x-2)(x-3)\cdots(x-k+1)}{k!}$.

Definition 2.1. Given $v_1, v_2, v_3, ..., v_n \in \mathbb{C}$, a *positive linear combination* of these numbers is any expression of the form $b_1v_1 + b_2v_2 + b_3v_3 + \cdots + b_nv_n$ for non-negative integers $b_1, b_2, b_3, ..., b_n$.

We define a *positive linear span*, $\mathbb{Z}^+(v_1, v_2, ..., v_n) \in \mathbb{C}$ to be the set of all positive linear combinations of a given set of numbers.

Now, we can define $R_+(S)$.

Definition 2.2. Let $S \in \mathbb{C}$. We define $R_+(S)$ as the positive linear span $\mathbb{Z}^+\left(\binom{S}{0}, \binom{S}{1}, \binom{S}{2}, ...\right)$.

We now prove some basic properties of $R_+(S)$.

Lemma 2.1. *$R_+(S)$ is a closed ring under multiplication.*

Proof. In order to prove the lemma, it's sufficient to show that the product of $\binom{r}{i}$ and $\binom{r}{j}$ can be expressed as a positive linear combination of $\binom{r}{k}$ for some k. This specifically follows from the fact that $(1+z)^r(1+w)^r = (1+(z+w+zw))^r$. We can expand this to get $\Sigma_{i,j}\binom{r}{i}\binom{r}{j}z^iw^j = \Sigma_k\binom{r}{k}(z+w+zw)^k$. It follows that $\binom{r}{i}\binom{r}{j}$ is equal to the coefficient of z^iw^j in $\Sigma_k\binom{r}{k}(z+w+zw)^k$, which is a positive linear combination of $\binom{r}{k}$ since all coefficients in the expansion of $(z+w+zw)^k$ are positive integers. □

Lemma 2.2. *If $t \in R_+(S)$ and $t' \in R_+(t)$, then $t' \in R_+(S)$.*

Proof. This follows from Lemma 1.1 in the introduction as well as [2]. □

The main objective of our research is to study $R_+(S)$ for some values of S.

We can easily figure out $R_+(S)$ for integer S.

Theorem 2.3. *For integer values of S, there are two possible cases for $R_+(S)$. If $S \geq 0$, then $R_+(S)$ is all positive integers. If $S < 0$, then $R_+(S)$ is all integers.*

Proof. First consider the case of $S \geq 0$.

Note that $\binom{S}{k} = 0$ if $S < k$.

Thus, we are looking at $\mathbb{Z}^+\left(\binom{S}{0}, \binom{S}{1}, ..., \binom{S}{S}\right)$. The numbers $\left(\binom{S}{0}, \binom{S}{1}, ..., \binom{S}{S}\right)$, are all integers greater than zero, which implies we can't achieve any negative integers in our span. We can use the number $\binom{S}{0} = 1$ to span all positive integers.

Then, we look at the case of $S < 0$.

Lemma 2.4. *For $S < 0$, it holds that $\mathbb{Z}^+\left(\binom{S}{0}, \binom{S}{1}\right) = \mathbb{Z}$.*

Proof. We know that $\binom{S}{0} = 1$ and $\binom{S}{1} = S$, a negative number. We can add $(-S-1)\cdot 1$ and S to get -1. Then, we can use 1 and -1 as generators to create the entirety of $\mathbb{Z}$. □

Since all $\binom{S}{k}$ are integers, we conclude from the statement of our lemma that $R_+(S) = \mathbb{Z}$ for $S < 0$. □

2.1 Facts about $\mathbb{Z}/p^q\mathbb{Z}$

It's useful for us to now show a few properties of $\mathbb{Z}/p^q\mathbb{Z}$ for prime p. These facts will be used in later proofs.

Lemma 2.5. *Multiplication by n such that $p \nmid n$ maps $\mathbb{Z}/p^q\mathbb{Z}$ to $\mathbb{Z}/p^q\mathbb{Z}$ bijectively.*

Proof. Denote the map of multiplication by n $f : \mathbb{Z}/p^q\mathbb{Z} \to \mathbb{Z}/p^q\mathbb{Z}$. Let's start with proving that f is injective. Given elements $x_1, x_2 \in \mathbb{Z}/p^q\mathbb{Z}$, we want to show that iff $f(x_1) = f(x_2)$, then $x_1 = x_2$.

If $f(x_1) = f(x_2)$, then we get that $n \cdot x_1 \equiv n \cdot x_2 \pmod{p^q}$. Thus, $n(x_1 - x_2) \equiv 0 \pmod{p^q}$, and as $\gcd(n, p) = 1$, we get $x_1 \equiv x_2 \pmod{p^q}$ and $x_1 = x_2$ as elements of $\mathbb{Z}/p^q\mathbb{Z}$.

Next, we prove that f is surjective.

Since we know that f is injective, we know that each $a \in \mathbb{Z}/p^q\mathbb{Z}$ maps to a unique element of $\mathbb{Z}/p^q\mathbb{Z}$. So it follows that the image of f has p^q unique elements. However, we know that $|\mathbb{Z}/p^q\mathbb{Z}| = p^q$, hence the image of f has to cover the whole $|\mathbb{Z}/p^q\mathbb{Z}|$. This shows that f is surjective, and the fact that f is bijective follows. □

Lemma 2.6. *Any equation of the form* $x^2 - m$ *for* $m \in \mathbb{Z}$ *has exactly* 2 *solutions in* $\mathbb{Z}/p^q\mathbb{Z}$ *for* p $\neq 2$ *if the Legendre symbol* $\left(\dfrac{m}{p}\right)$ *is equal to* 1.

Proof. We use induction on q. In the base case of $q = 1$, this is true by the definition of the Legendre symbol.

For the inductive step, assume that there are exactly 2 solutions in $\mathbb{Z}/p^q\mathbb{Z}$, namely n_1 and n_2.

Since a solution in $\mathbb{Z}/p^{q+1}\mathbb{Z}$ must be a solution in $\mathbb{Z}/p^q\mathbb{Z}$, we know that all solutions in $\mathbb{Z}/p^{q+1}\mathbb{Z}$ are of the form $n_i + kp^q$ where $k \in \mathbb{N}$ ranges from 0 to $p - 1$ and $i = 1, 2$.

We now check if these are solutions to the equation $x^2 - m \equiv 0 \pmod{p^{q+1}}$. Substituting, we have $n_i^2 + 2n_ikp^q + k^2p^{2q} \equiv m \pmod{p^{q+1}}$. This is equivalent to $n_i^2 + 2n_ikp^q \equiv m \pmod{p^{q+1}}$. We also have that $n_i^2 \equiv m \pmod{p^q}$, so $n_i^2 \equiv m + l_ip^q \pmod{p^{q+1}}$ and $l_i \in \mathbb{N}$ such that $0 \leq l_i < p$. After plugging this in, we finally have $l_ip^q + 2n_ikp^q \equiv 0 \pmod{p^{q+1}}$. As $p \nmid n_i$, Lemma 2.5 tells us that there exists exactly 1 solution for each n_i, so there are 2 total solutions for the original equation. □

3 S is rational

We now consider $R_+(S)$ for rational S.

Theorem 3.1. *For rational values of $S = \frac{m}{n}$, $R_+(S)$ is equal to $\mathbb{Z}[\frac{1}{n}] = \mathbb{Z}[\frac{m}{n}]$.*

In order to prove this theorem, we need to first prove a few lemmas.

Proposition 3.2. *All numbers of the form $\binom{\frac{m}{n}}{k}$ can be written in the form of $\frac{M}{n_1^{l_1}\cdot n_2^{l_2}\cdot\dots\cdot n_n^{l_n}}$ where $n_1, n_2, ..., n_n$ are prime factors of n.*

Proof. Using the definition for $\binom{x}{k}$, we have

$$\binom{\frac{m}{n}}{k} = \frac{\frac{m}{n}\cdot(\frac{m}{n}-1)\cdot(\frac{m}{n}-2)\dots(\frac{m}{n}-k+1)}{k!}$$

. Multiplying the numerator and denominator by n^k, we get $\frac{m(m-n)(m-2n)...(m-(k-1)n)}{n^k\cdot k!}$.

Denote the numerator of the above fraction, $x_k = m(m-n)(m-2n)\dots(m-(k-1)n)$.

Furthermore, define the p-adic valuation of a number x, written as $\nu_p(x)$, to be the largest exponent of p that divides x.

Now, we will show that for all primes p such that $p \nmid n$, $\nu_p(x_k) \geq \nu_p(k!)$.

In order to find $\nu_p(x_k)$, we denote the terms of x_k in the following way: $a_0 = m$, $a_1 = m-n$, $a_2 = m-2n$ and more generally, $a_i = m - ni$. Note that in each set of p consecutive terms, $\{a_0, a_1, ..., a_{p-1}\}$, $\{a_p, a_{p+1}, ..., a_{2p-1}\}$, and more generally, $\{a_{ip}, a_{ip+1}, ..., a_{p(i+1)-1}\}$, it is obvious by Lemma 2.5 that there is 1 term divisible by p where $p \nmid n$. Thus among a_i, there are at least $\lfloor\frac{k}{p}\rfloor$ numbers divisible by p in the first k terms.

Given the set of remainders modulo p^q, $\{p^q i \pmod{p^q}, ..., p^q(i+1)-1 \pmod{p^q}\}$, this is equivalent to $\mathbb{Z}/p^q\mathbb{Z}$.

From our Lemma 2.5, we have that $\{np^q i \pmod{p^q}, \dots, n(p^q(i+1)-1) \pmod{p^q}\}$ is also equivalent to $\mathbb{Z}/p^q\mathbb{Z}$.

We can shift each term by $-m$ to get $\{np^q i - m \pmod{p^q}, ..., n(p^q(i+1)-1) - m \pmod{p^q}\}$ which is also equivalent to $\mathbb{Z}/p^q\mathbb{Z}$, since $\mathbb{Z}/p^q\mathbb{Z}$ is a group under addition..

From this, it follows that the set contains 0, so among $\{a_{p^q i}, ..., a_{p^q(i+1)-1}\}$, one number is divisible by p^q and thus, there are at least $\lfloor \frac{k}{p^q} \rfloor$ numbers divisible by p^q in the first k terms.

However, in the first k positive integers, there are exactly $\lfloor \frac{k}{p^q} \rfloor$ numbers divisible by p^q.

We now have that $\nu_p(x_k) \geq \nu_p(k!)$. From this, it follows that if $p \nmid n$, then there are no factors of it in the denominator after simplification, since there are enough powers of p in the numerator to cancel out all the powers of p in $k!$. □

Lemma 3.3. *For m, n co-prime, $\mathbb{Z}[\frac{1}{n}] = \mathbb{Z}[\frac{m}{n}]$.*

Proof. In order to show this, we need to show that $\mathbb{Z}[\frac{m}{n}] \subseteq \mathbb{Z}[\frac{1}{n}]$ and $\mathbb{Z}[\frac{1}{n}] \subseteq \mathbb{Z}[\frac{m}{n}]$. The first part is obvious. For the second part, note that Bezout's identity tells us that there exist positive integer solutions to the equation $Am + Bn = 1$ for integers A, B. Dividing by n, we get $A\frac{m}{n} + B = \frac{1}{n}$ which means that $\frac{1}{n} \in \mathbb{Z}[\frac{m}{n}]$. It immediately follows then that $\mathbb{Z}[\frac{1}{n}] \subseteq \mathbb{Z}[\frac{m}{n}]$. □

Lemma 3.4. *For $S \in \mathbb{Q}$, we have $R_+(S) \subseteq \mathbb{Z}[S]$.*

Proof. Let $S = \frac{m}{n}$ for relatively prime positive integers m, n. We will instead prove that $R_+(S) \subseteq \mathbb{Z}[\frac{1}{n}]$ (Lemma 3.3).

By Proposition 3.2, we get that all numbers of the form $\binom{\frac{m}{n}}{k}$ can be written in the form of $\frac{M}{n_1^{l_1} \cdot n_2^{l_2} \cdot \dots \cdot n_n^{l_n}}$ where $n_1, n_2, ..., n_n$ are prime factors of n. Since we can write this number in the form, $\frac{M'}{n^\alpha}$ where $\alpha, M' \in \mathbb{Z}$ this number is in $\mathbb{Z}[\frac{1}{n}]$ as we can take $\frac{1}{n}$, raise it to the αth power, and multiply by M'. It follows that $\binom{\frac{m}{n}}{k} \in \mathbb{Z}[\frac{1}{n}]$ and thus $R_+(S) \subseteq \mathbb{Z}[S]$. □

Lemma 3.5. *For $S \in \mathbb{Q}$, we have $\mathbb{Z}[S] \subseteq R_+(S)$.*

Proof. If we can show that $1, \frac{m}{n}, -1 \in R_+(\frac{m}{n})$, then we can show that $\mathbb{Z}[S] \subseteq R_+(S)$. Indeed take $y \in \mathbb{Z}[\frac{m}{n}]$, we have $y = \sum y_i \left(\frac{m}{n}\right)^i$ where y_i are integers. Since $R_+(S)$ is closed under addition, it's sufficient to show that each term belongs to $R_+(S)$. To create each term, raise

$\frac{m}{n}$ to the i-th power and if $y_i \geq 0$, multiplied by y_i. If $y_i < 0$, then we multiply by -1 and $-y_i$.

We have $\binom{\frac{m}{n}}{0} = 1$ and $\binom{\frac{m}{n}}{1} = \frac{m}{n}$, so $1, \frac{m}{n} \in R_+(\frac{m}{n})$.

From Proposition 3.2, we have that all numbers of the form $\binom{\frac{m}{n}}{k}$ can be written as $\frac{M}{n_1^{l_1} \cdot n_2^{l_2} \cdot \dots \cdot n_n^{l_n}}$ where $n_1, n_2, ..., n_n$ are prime factors of n. Also, note that there exists k such that $\binom{\frac{m}{n}}{k} < 0$ since we can simply take the first k such that $k > \frac{m}{n}$ if $\frac{m}{n}$ is positive and $k = 1$ otherwise.

For such a k, then consider $\frac{M}{n_1^{l_1} \cdot n_2^{l_2} \cdot \dots \cdot n_n^{l_n}} \cdot n_1^{l_1} \cdot n_2^{l_2} \cdot \dots \cdot n_n^{l_n} + (-M - 1) = -1$ (which works as $(-M - 1)$ is positive) and thus, $-1 \in R_+(\frac{m}{n})$. □

Now, we can finally prove Theorem 3.1, $R_+(S) = \mathbb{Z}[\frac{1}{n}] = \mathbb{Z}[\frac{m}{n}]$.

Proof. From Lemma 3.3, we have that $\mathbb{Z}[\frac{1}{n}] = \mathbb{Z}[\frac{m}{n}]$ Lemma 3.4 tells us that $R_+(\frac{m}{n}) \subseteq \mathbb{Z}[\frac{m}{n}]$. Lemma 3.5 tells us that $\mathbb{Z}[\frac{m}{n}] \subseteq R_+(\frac{m}{n})$. Combining these lemmas, we finally have that $R_+(\frac{m}{n}) = \mathbb{Z}[\frac{m}{n}] = \mathbb{Z}[\frac{1}{n}]$ □

We now define the notion of an algebraic number.

Definition 3.1. [3] A complex number ξ is called an *algebraic number* if it satisfies some polynomial equation $f(x) = 0$ where $f(x)$ is a polynomial over $\mathbb{Q}$.

We know that all rational numbers $\frac{m}{n}$ are algebraic, they are roots of polynomials of the form $nx - m = 0$. It's natural then to try to calculate $R_+(S)$ for more general algebraic numbers, which is the goal of our research.

4 $S = \sqrt{n}$

In this section, we take S to be of the form, $\sqrt{n}$ for nonsquare $n > 0$.

We calculate $R_+(S)$ for $S = \sqrt{n}$.

Theorem 4.1. *We have $\mathbb{Z}[\sqrt{n}] \subset R_+(\sqrt{n})$ for nonsquare $n > 0$.*

In order to prove this theorem, we need to first prove a few lemmas.

Lemma 4.2. *All numbers of the form $\binom{\sqrt{n}}{k}$ can be expressed in the form $a_k - b_k\sqrt{n}$ for even k or $c_k\sqrt{n} - d_k$ for odd k where a_k, b_k, c_k, d_k are non-negative rational numbers.*

Proof. We prove this by induction. The base cases of $k = 0$ and $k = 1$ give values of 1 and $\sqrt{n}$ respectively.

Now for the inductive step. Note that $\binom{\sqrt{n}}{k+1}$ equals $\binom{\sqrt{n}}{k} \cdot \frac{\sqrt{n}-k}{k+1}$. Take k to be odd. We have the number $\binom{\sqrt{n}}{k}$ to be of the form $c_k\sqrt{n} - d_k$, and the next number for even k is of the form $\frac{nc_k+kd_k}{k+1} - \frac{(d_k+kc_k)\sqrt{n}}{k+1}$. Take k to be even. We have $\binom{\sqrt{n}}{k}$ of the form $a_k - b_k\sqrt{n}$, and the next $\binom{\sqrt{n}}{k+1}$ is of the form $\frac{(a_k+kb_k)\sqrt{n}}{k+1} - \frac{nb_k+ka_k}{k+1}$.

In both cases, k is odd and k is even, we have a $\binom{\sqrt{n}}{k+1}$ of the desired form, so we are done. □

Let $\frac{a_k}{b_k} = h_k$ for even k and $\frac{d_k}{c_k} = h_k$ for odd k.

Lemma 4.3. *If there is an h_{2j+1} that is larger than h_{2i} for $i, j \in \mathbb{N}$, then $-\sqrt{n} \in R_+(\sqrt{n})$.*

Proof. Let's take a linear combination of $a_{2i} - b_{2i}\sqrt{n}$ and $c_{2j+1}\sqrt{n} - d_{2j+1}$. Multiply the first equation by d_{2j+1}, the second by a_{2i} and add them.

We thus have $(a_{2i}c_{2j+1} - b_{2i}d_{2j+1})\sqrt{n}$. If $b_{2i}d_{2j+1} > a_{2i}c_{2j+1}$ (this is equivalent to $h_{2j+1} > h_{2i}$), we get a negative rational multiple (say $-\frac{M}{N}$ for positive integer M, N) of $\sqrt{n}$. We can then multiply by N and add $(M-1)\sqrt{n}$ to get the desired $-\sqrt{n}$. □

Lemma 4.4. *We can get a recursive formula for h_j for positive integers j. Namely $h_{j+1} = \frac{jh_j+n}{h_j+j}$ for $j \geq 2$ with $h_2 = n$.*

Proof. We show this is true for j is odd and j is even. If j is odd, then we have $h_{j+1} = \frac{a_{j+1}}{b_{j+1}} = \frac{c_j n + j d_j}{d_j + j c_j} = \frac{j h_j + n}{h_j + j}$ as $a_{j+1} = \frac{c_j n + j d_j}{j+1}$ and $b_{j+1} = \frac{d_j + j c_j}{j+1}$. If j is even, then we have $h_{j+1} = \frac{d_{j+1}}{c_{j+1}} = \frac{b_j n + j a_j}{a_j + j b_j} = \frac{j h_j + n}{h_j + j}$ as $d_{j+1} = b_j n + j a_j$ and $c_{j+1} = a_j + j b_j$. □

Let $m_j = h_j - \sqrt{n}$. Note that m_j is positive if $h_j \geq \sqrt{n}$ and negative if $h_j < \sqrt{n}$.

Lemma 4.5. *The sequence m_j is monotonic for $j > \sqrt{n}$.*

Proof. Take the difference $h_{j+1} - h_j = \frac{n - h_j^2}{h_j + j}$.

This means that we have $h_{j+1} > h_j$ iff $h_j < \sqrt{n}$.

Calculate $m_{j+1} = \frac{m_j (j - \sqrt{n})}{m_j + \sqrt{n} + j}$.

For $j > \sqrt{n}$, we know that m_{j+1} has the same sign as m_j. As $j+1$, $j+2$, and so on are all greater than $\sqrt{n}$, we get a chain of terms all of the same sign after $j > \sqrt{n}$.

Thus after $j > \sqrt{n}$, we have all $h_j > \sqrt{n}$ ($m_j > 0$) or $h_j < \sqrt{n}$ ($m_j < 0$), so h_j is monotonic after $j > \sqrt{n}$. □

Proposition 4.6. $-\sqrt{n} \in R_+(S)$

Proof. Given that the sequence is monotonic after $j > \sqrt{n}$, it is true that we can simply choose any pair of consecutive terms after $j > \sqrt{n}$ such that the term with odd j is greater than the term with even j. If the sequence is increasing, simply take h_{2n}, h_{2n+1} for $2n > \sqrt{n}$. If the sequence is decreasing, simply take h_{2n+1}, h_{2n+2} for $2n > \sqrt{n}$. □

Recall that we are trying to show $\mathbb{Z}[\sqrt{n}] \subset R_+(\sqrt{n})$ for nonsquare $n > 0$.

Proof. Note that if we show $1, \sqrt{n}, -1, -\sqrt{n} \in R_+(S)$, then it is sufficient to conclude that $\mathbb{Z}[\sqrt{n}] \subset R_+(S)$. Indeed, from this using positive linear combinations, we can get any $a + b\sqrt{n}$.

We have $\binom{\sqrt{n}}{0} = 1$ and $\binom{\sqrt{n}}{1} = \sqrt{n}$. From the conclusion of Proposition 4.6, we have that $-\sqrt{n} \in R_+(S)$. To get -1, we take $\sqrt{n} \cdot -\sqrt{n}$ and add $n - 1$ (a positive number). □

4.1 Denominators of fractions of the form $\binom{\sqrt{2}}{k}$

We now consider the fractions $\binom{\sqrt{2}}{k}$ where k is a natural number.

From Lemma 4.2, we know all numbers of this form can be expressed as $a_k - b_k\sqrt{2}$ for even k or $c_k\sqrt{2} - d_k$ for odd k where a_k, b_k, c_k, d_k are non-negative rational numbers.

We can combine these numbers into simplified fractions over the denominator, and we are specifically interested in the prime factors of these denominators.

Before we proceed, we need some more definitions of some concepts in algebraic number theory.

The general concept of an algebraic field is as follows.

Definition 4.1. [3] An *algebraic field* is any subset of the set of all algebraic numbers which is a field itself.

Then, we define algebraic integers.

Definition 4.2. [3] An algebraic number ξ is called an *algebraic integer* if it satisfies some monic polynomial equation $f(x) = x^n + b_1x^{n-1} + \cdots + b_n = 0$ with integral coefficients.

Now, we move on to the definition of a norm.

Definition 4.3. [3] Denote the norm $N(\alpha)$ of a number $\alpha = (a + b\sqrt{m})/c$ in $\mathbb{Q}(\sqrt{m})$ as the product of α and its conjugate. Thus, we have $N(\alpha) = \frac{a^2-b^2m}{c^2}$.

A *unit* is defined as an element having norm 1. It is known that all units are invertible.

Furthermore, we need the definition of an associate.

Definition 4.4. Two numbers are *associated* in an algebraic field if they differ by multiplication by a unit.

Finally, we can define primes in an algebraic field.

Definition 4.5. An *algebraic integer* α, not a unit, in a quadratic field $\mathbb{Q}(\sqrt{m})$ is called prime if it is divisible by only its associates and the units of the field.

We now move on to the classification of primes.

Proposition 4.7. *(Theorem 9.29 in [3]) Primes in* $\mathbb{Q}(\sqrt{2})$ *are given by:* p *for* $\left(\frac{2}{p}\right) = -1$, *pairs* $p_1 \neq p_2$ *such that* $N(p_1) = N(p_2) = p = p_1 p_2$, *for* $\left(\frac{2}{p}\right) = 1$, $\sqrt{2}$, *and all their associated primes.*

After these definitions, we move on to the main theorem we want to prove in this section.

Theorem 4.8. *Denominators of the simplified fraction* $\binom{\sqrt{2}}{k}$ *where* $k \in \mathbb{N}$ *only contain multiples of primes* p *such that* $\left(\frac{2}{p}\right) = 0, -1$.

We start by proving a lemma.

Lemma 4.9. *The sum* $\Sigma_{i=0}^{k-1} \nu_p[N(\sqrt{2} - i)]$ *is more than* 2 *times* $\nu_p(k!)$.

Proof. We want to show inductively that for $q \geq 1$, there are at least 2 times $\lfloor \frac{k}{p^q} \rfloor$ factors of p^q in the numerator. This is shown if we can say that there are exactly 2 solutions to $x^2 - 2 \pmod{p^q}$ from ip^q to $(i+1)p^q - 1$ for any i.

This is true by Lemma 2.6. □

From the previous lemma, we know that the denominator of the norm of the fraction $\binom{\sqrt{2}}{k}$ has no factors of p. Now, we want to show it for the fraction itself.

Lemma 4.10. *If* L_1 *and* L_2 *are two integers from* ip^q *to* $(i+1)p^q - 1$ *such that* $p^q | N(\sqrt{2} - L_1)$ *and* $p^q | N(\sqrt{2} - L_2)$ *(which exist from the previous lemma), then* $(\sqrt{2} - L_1)(\sqrt{2} - L_2)$ *is divisible by* p^q.

Proof. Expanding, we want to now show that $2 - \sqrt{2}(L_1 + L_2) + L_1 L_2$ is divisible by p^q. As L_1 and L_2 are solutions to $x^2 - 2 = 0$ in $\mathbb{Z}/p^q\mathbb{Z}$, it follows that $L_1 \equiv -L_2 \pmod{p^q}$. Then we get that $L_1 + L_2 \equiv 0 \pmod{p^q}$ and $L_1 L_2 \equiv -2 \pmod{p^q}$, so we are done. □

Now we can prove Theorem 4.8.

Proof. From Lemma 4.10, we get that $(\sqrt{2}-L_1)(\sqrt{2}-L_2)$ is divisible by p^q. From a similar reasoning to Proposition 3.2, there are enough factors of p in the numerator to cancel all the factors of p in the denominator. □

After showing this, we can say that there are no powers of p such that $\left(\frac{2}{p}\right) = 1$ in the denominator of the simplified fraction $\binom{\sqrt{2}}{k}$.

Now, we want to more generally calculate $R_+(\sqrt{2})$.

Theorem 4.11. *$R_+(\sqrt{2}) = \mathbb{Z}[\frac{1}{p_1}, \frac{1}{p_2}, \frac{1}{p_3}, ..., \frac{1}{p_i}, ...][\sqrt{2}]$ for all p_i such that $\left(\frac{2}{p_i}\right) \neq 1$.*

Proof. We first show that $R_+(\sqrt{2}) \subset \mathbb{Z}[\frac{1}{p_1}, \frac{1}{p_2}, \frac{1}{p_3}, \dots \frac{1}{p_i}, \dots][\sqrt{2}]$ for p_i such that $\left(\frac{2}{p_i}\right) \neq 1$. This is true from Theorem 4.8.

To show $\mathbb{Z}[\frac{1}{p_1}, \frac{1}{p_2}, \frac{1}{p_3}, \dots \frac{1}{p_i}, \dots][\sqrt{2}] \subset R_+(\sqrt{2})$, we just need to show $1, -1, \sqrt{2}, \frac{1}{p_1}, \frac{1}{p_2}, \dots, \frac{1}{p_i}, \dots \in R_+(\sqrt{2})$.

Lemma 4.12. *The numerator of the simplified fraction $\binom{\sqrt{2}}{k}$ contains no powers of primes p such that $\left(\frac{2}{p}\right) = -1$.*

Proof. This follows from the fact that $N(\binom{\sqrt{2}}{k}$ has no factors of p as $n^2 - 2 \neq 0 \pmod{p}$ which is in fact equivalent to saying $\left(\frac{2}{p}\right) = -1$. □

Given p such that $\left(\frac{2}{p}\right) = -1$. Because of Lemma 4.12, it's true that in the simplified fraction $\binom{\sqrt{2}}{p}$, there are no factors of p in the numerator that can cancel the factor of p in the denominator.

We get that $\binom{\sqrt{2}}{p}\binom{-\sqrt{2}}{p} = N(\binom{\sqrt{2}}{p}$ which is equivalent to some fraction $\frac{M}{Np^2}$ for relatively prime M, N.

We gather that $\frac{1}{p} \in R_+(\frac{M}{Np^2}$ from Theorem 3.1. We also have that $\frac{M}{Np^2} \in R_+(\sqrt{2})$ by Lemma 2.2. This means that $\frac{1}{p} \in R_+(\sqrt{2})$.

This concludes the proof. □

5 Acknowledgments

I'd like to thank Daniil Kalinov of the MIT Math Department for mentoring me throughout the course of my project, meeting daily with me, and teaching me mathematics. I'd also like to thank Dr. Tanya Khovanova for her advice regarding project direction and role as head mentor. I would also like to thank Jessica Shi and Gary Lee for their tutorship and thoughtful advice regarding my paper writing and presentation. I also want to thank the Department of Defense, Dr. Michael C. Mintzer and Ms. Alla R. Zaprudsky, and Dr. and Mrs. Jong K. Lee for sponsoring me and providing me with financial support. Another thank you goes to MIT, CEE, and RSI for providing me with this wonderful opportunity. Finally, I'd like to thank my wonderful friends here who have morally supported me and helped me throughout the entire process.

References

[1] K. Conrad. On the origin of representation theory. *Enseignement Mathematique*, 44:361–392, 1998.

[2] N. Harman and D. Kalinov. Classification of simple algebras in Deligne category $\mathrm{Rep}(S_t)$. *arXiv preprint arXiv:1901.05080*, 2019.

[3] I. Niven. *An Introduction to the Theory of Numbers*. John Wiley & Sons Inc., Canada, 1991.