A SHORT INTRODUCTION TO RINGS OF INTEGERS

PLOY WATTANAWANICHKUL

Abstract. This paper presents a brief introduction to rings of integers, starting from the definitions and fundamental properties of algebraic numbers and algebraic integers. Then, we provide some examples of rings of integers including rings of integers of a cyclotomic number field and rings of quadratic integers. Lastly, we show how the knowledge in this topic can be applied to solving interesting mathematics problems.

1. Introduction

Let us start from the two fundamental objects, *algebraic numbers* and *algebraic numbers.*

Definition 1.1. *Algebraic numbers are those numbers that satisfy an equation of the form*

$$x^n + a_n x^{n-1} + \cdots + a_1 x + a_0 = 0, \tag{1.1}$$

where the coefficients are rational numbers. When the coefficients are integers ($a_i \in \mathbb{Z}$)*, the algebraic number x is called an algebraic integer.*

Remark 1.2. *Definition 1.1 may alternatively state that a root of $a_n x^n + a_n x^{n-1} + \cdots + a_1 x + a_0 = 0$, where $a_i \in \mathbb{Z}$ is called an algebraic number while a root of the same equation with $a_n = 1$ is an algebraic integer.*

Remark 1.3. *All rational numbers are algebraic numbers because for any rational number a/b, where $a, b \in \mathbb{Z}, (a, b) = 1$, a/b is a root of equation $bx - a = 0$. In particular, the only rational numbers that are algebraic integers, i.e. the answer of monic linear polynomials $\in \mathbb{Z}[x]$, are the integers. Thus, this is a reason why we call them algebraic integers!*

For better understanding of *algebraic numbers* and *algebraic integers*, consider the following examples.

- The roots of quadratic polynomial $ax^2 + bx + c$ with integer coefficients a, b, and c are algebraic numbers. If the quadratic polynomial is monic, i.e., $a = 1$, then the roots are qualified as algebraic integers. There are also special names to these kinds of numbers, namely, quadratic numbers and quadratic integers, respectively.
- Some irrational numbers are algebraic numbers and some are not. For example, the numbers $\sqrt{7}$ and $\frac{\sqrt[3]{7}}{2}$ are algebraic since they are roots of polynomials $x^2 - 7$ and $343x^3 - 2$, respectively.

Date: August 2, 2021.

- The golden ratio ϕ is algebraic number since ϕ is a root of the polynomial $x^2 - x - 1$.
- The numbers π and e are not algebraic numbers, and we call non-algebraic numbers are *transcendental numbers.*

Algebraic numbers and algebraic integers have nice and well-studied properties that we would like to note here without proving.

Theorem 1.4. *The algebraic numbers form* ***a field*** *because the sum, difference, product and quotient with nonzero denominator of two algebraic numbers is always algebraic. Besides, every root of a polynomial equation whose coefficients are algebraic is again algebraic. This can be rephrased as the field of algebraic numbers is "algebraically closed."*

Theorem 1.5. *From Remark 1.3, we know that algebraic integers comprises a proper superset of the integers. Also, similarly to Proposition 1.4, the sum, difference, product, but not quotient, of algebraic integers are again algebraic integers, which means that the algebraic integers form* ***a ring****.*

With all the definitions and properties we noted in this section, we are now ready to define the main object in this paper, *rings of integers.*

2. Rings of Integers

Definition 2.1. *(Rings of Integers) Given an algebraic number field K, the ring of integers of field K is then the ring of all integral elements contained in K, i.e., those that are roots of some monic polynomial with integer coefficients, $x^n + c_{n-1}x^{n-1} + \cdots + c_0$. This ring is often denoted by $\mathcal{O}_k$.*

Remark 2.2. *Since the set of integers belongs to any K and is an integral element of K, the ring $\mathbb{Z}$ is always a subring of $\mathcal{O}_k$ In other words, the ring of integers $\mathbb{Z}$ is the simplest possible ring of integers, namely, $\mathbb{Z} = \mathcal{O}_{\mathbb{Q}}$ where $\mathbb{Q}$ is the field of rational numbers.*

While the algebraic integers in any number field are in many ways analogous to the integers, one difference that is worth pointing out is its multiplicative structure.

In a ring of integers, every element has a factorization into irreducible elements, but the ring does not have to have the property of unique factorization. One classic example is the ring of integers $\mathbb{Z}[\sqrt{-5}]$. The element 6 in this ring has two distinct factorizations into irreducibles, namely

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Let us now observe some examples of rings of integers, namely, the ring of integers of a cyclotomic number field and the ring of integers of a quadratic number field.

Definition 2.3. *(Ring of integers of a cyclotomic number field) If p is a prime, ζ is a p-th root of unity and $K = \mathbb{Q}(\zeta)$ is the corresponding cyclotomic field, then $\mathcal{O}_K = \mathbb{Z}[\zeta]$ defines the ring of integers of K, whose basis is given by $(1, \zeta, \zeta^2, \ldots, \zeta^{p-2})$.*

Notice that the above basis of $\mathbb{Z}[\zeta]$ is $(1, \zeta, \zeta^2, \ldots, \zeta^{p-2})$, not including ζ^{p-1} as one might expect. This fact indeed corresponds to a point we discussed in class, which we present again in the following exercise.

Exercise 2.4. *Let ζ_3 denote a nontrivial cube root of 1 (i.e., $\zeta_3^3 = 1$ and $\zeta_3 \neq 1$). Find $[\mathbb{Q}(\zeta_3) : \mathbb{Q}]$ and a basis for $\mathbb{Q}(\zeta_3)$ over $\mathbb{Q}$.*

Solution. It is quite clear that any element of $\mathbb{Q}(\zeta_3)$ can be written in the form $a_1 + a_2\zeta_3 + a_3\zeta^2$, where $a_1, a_2, a_3 \in \mathbb{Q}$. However, $1, \zeta_3, \zeta_3^2$ are not linearly independent. This is because

$$1 - \zeta_3^3 = 0 \implies (1 - \zeta_3)(1 + \zeta_3 + \zeta_3^2) = 0,$$

so, since $\zeta_3 \neq 1$, $1+\zeta_3+\zeta_3^2$ must be 0. In other words, ζ_3^2 can be written as $-1-\zeta_3$. Hence, a basis of this ring of cyclotomic integers is $(1, \zeta_3)$ and $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$. □

Definition 2.5. *(Ring of integers of a quadratic number field) If d is a square-free integer and $K = \mathbb{Q}(\sqrt{d})$ is the corresponding quadratic field, then $\mathcal{O}_K$ is a ring of quadratic integers and its integral basis is given by*

$$\begin{cases} (1, \sqrt{d}), & \textit{if } d \equiv 2, 3 \pmod 4, \\ (1, \frac{1+\sqrt{d}}{2}), & \textit{if } d \equiv 1 \pmod 4. \end{cases}$$

Since it is not so intuitive why the basis appears to be different given distinct d modulo 4, we would like to take time investigating this kind of integer ring in depth in the next section.

3. Rings of Quadratic Number Fields

Before we show why an integral basis of $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{d})$, can be given like in Definition 2.5, let us observe the following proposition that is also essential.

Proposition 3.1. *Suppose $d \neq 1$ is square-free. Then the numbers*

$$x + y\sqrt{d} \ (x, y \in \mathbb{Q})$$

form a quadratic number field $\mathbb{Q}(\sqrt{d})$. Moreover, every quadratic number field is of this from; and different square-free integers, $d, d' \neq 1$ give rise to different quadratic number fields.

Proof. First, recall the classic proof that $\sqrt{d}$ is irrational.

$$\sqrt{d} = \frac{m}{n} \Longrightarrow n^2 d = m^2,$$

so if any prime divides d, it would divide n^2d to an odd power while dividing m^2 to an even power. Contradiction.

Now, we prove that the numbers $x + y\sqrt{d}$ form a field. It is clear that the numbers $x + y\sqrt{d}$ form a commutative ring. Then, we show that every element has its multiplicative inverse.

$$\begin{aligned}\frac{1}{x+y\sqrt{d}} &= \frac{x-y\sqrt{d}}{(x-y\sqrt{d})(x+y\sqrt{d})}\\ &= \frac{x-y\sqrt{d}}{x^2-dy^2}\end{aligned}$$

Thus, it follows that these numbers form a field, and the degree of the field is 2 since $1, \sqrt{d}$ form a basis for the vector space.

Conversely, suppose F is a quadratic number field, where $1, \theta$ be a basis for the vector space. Then, θ satisfies a quadratic equation

$$a\theta^2 + b\theta + c = 0,$$

where $a, b, c \in \mathbb{Q}$ and a, b, c are not 0 simultaneously. Since F is of degree 2, $a \neq 0$, and we can take $a = 1$. Thus,

$$\theta = \frac{-b \pm \sqrt{D}}{2},$$

with $D = b^2 - 4c$. Now, we can write $D = k^2 d$, where d is a square-free integer, with $k \in \mathbb{Q}$. It follows easily that $F = \mathbb{Q}(\sqrt{d})$.

Finally, if $d \neq d'$ then $\mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}(\sqrt{d'})$. This is because, if not, we can write $\sqrt{d'} = x + y\sqrt{d}$ for some $x, y \in \mathbb{Q}$. Thus, we would have

$$d' = x^2 + dy^2 + 2xy\sqrt{d}.$$

However, this implies that $\sqrt{d} \in \mathbb{Q}$ if $xy \neq 0$. Otherwise, if $y = 0$, $\sqrt{d'} = x \in \mathbb{Q}$, or if $x = 0$, $d' = dy^2$ which is impossible as d and d' are square-free. □

Now, let us prove integral bases of $K = \mathbb{Q}(\sqrt{d})$ are as stated in Definition 2.5. To do so, recall that our goal is to find which number $x+y\sqrt{d}$ are algebraic integers and what elements span the set of those numbers. The statement we want to prove is indeed equivalent to the following theorem, which we prove it instead.

Theorem 3.2. *Let $\bar{\mathbb{Z}}$ denote the set of algebraic integers. Suppose*

$$z = x + y\sqrt{d} \in \mathbb{Q}\sqrt{d}.$$

Then,

(1) *If $d \not\equiv 1 \pmod 4$, $z \in \bar{\mathbb{Z}}$ if and only if $z = m + n\sqrt{d}$, where $m, n \in \mathbb{Z}$.*

(2) *If $d \equiv 1 \pmod 4$ $z \in \bar{\mathbb{Z}}$ if and only if $z = \dfrac{m + n\sqrt{d}}{2}$, where $m, n \in \mathbb{Z}$ and $m \equiv n \pmod 2$.*

Proof. If $z = x + y\sqrt{d} \in \bar{\mathbb{Z}}$, then $\bar{z} = x - y\sqrt{d} \in \bar{\mathbb{Z}}$ since z and $\bar{z}$ satisfy the same polynomial over $\mathbb{Q}$. Hence, $z + \bar{z} = 2x \in \bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. Also, $N(z) = z\bar{z} = x^2 - dy^2 \in \mathbb{Z}$. It follows that

$$4dy^2 = d(2y)^2 \in \mathbb{Z} \implies 2y \in \mathbb{Z}$$

since d is square-free. (For suppose $2y = p/q$, where $(p, q) = 1$. Then $dp^2/q^2 \in \mathbb{Z}$. If the prime $r|n$ then

$$r^2 | dp^2 \implies r^2 | d,$$

which is impossible since d is square-free.)

Thus, as we know $2x, 2y \in \mathbb{Z}$, we can write

$$z = \frac{m + n\sqrt{d}}{2},$$

where $m, n \in \mathbb{Z}$. Now

$$N(z) = \frac{m^2 - dn^2}{4} \in \mathbb{Z},$$

meaning $m^2 \equiv dn^2 \pmod 4$.

If n is even, then m is also even and vice versa, since d is square-free. On the other hand, if both m, n are odd, then $m^2 \equiv n^2 \equiv 1 \pmod 4$. It follows that $d \equiv 1 \pmod 4$.

In other words, if $d \not\equiv 1 \pmod 4$ then m, n are even, and so $z = a + b\sqrt{d}$, with $a, b \in \mathbb{Z}$.

On the other hand, if $d \equiv 1 \pmod 4$, then m, n are both even or both odd. It only remains to show that if $d \equiv 1 \pmod 4$ and m, n are both odd then

$$z = \frac{m + n\sqrt{d}}{2} \in \bar{\mathbb{Z}}.$$

It is sufficient to show that $\theta = \frac{1+\sqrt{d}}{2} \in \bar{\mathbb{Z}}$, since we can write $z = \frac{m-1}{2} + \frac{n-1}{2}\sqrt{d} + \theta$. Observe that $(\theta - 1/2)^2 = d/4$, i.e., $\theta^2 - \theta + (1-d)/4$. Since $d \equiv 1 \pmod 4$, $\theta \in \bar{\mathbb{Z}}$. □

4. Problems Related to Rings of Integers

In this section, we would like to discuss some problems related to rings of integers. The first problem is from one of Indian mathematics competitions.

Problem 4.1. *Prove that the number*

$$S = \sqrt{1001^2 + 1} + \sqrt{1002^2 + 1} + \cdots + \sqrt{2000^2 + 1}$$

is irrational.

Proof. We note that each number in the form $\sqrt{n^2 + 1}$ is an algebraic number as it is a root of $x^2 - (n^2 + 1)$. Then, by Theorem 1.4, we know that the sum of algebraic numbers is still an algebraic number.

Now, we prove that S is irrational by contradiction. Suppose that S is rational, then by Remark 1.3, we know that any algebraic integer that a rational must be an integer. In other words, S must be an integer.

Now, we note that if S is an integer, $S - 1001 - 1002 - \cdots - 2000$ must also be integer. However, as we know that

$$\sqrt{n^2 + 1} - n = (\sqrt{n^2 + 1} - n) \cdot \frac{\sqrt{n^2 + 1} + n}{\sqrt{n^2 + 1} + n} = \frac{1}{\sqrt{n^2 + 1} + n},$$

we have

$$\begin{aligned}
S-1001-1002-\cdots-2000 &= \sqrt{1001^2+1}-1001+\cdots+\sqrt{2000^2+1}-2000\\
&= \frac{1}{\sqrt{1001^2+1}+1001}+\cdots\frac{1}{\sqrt{2000^2+1}+2000}\\
&< \frac{1}{2\cdot 1001}+\cdots\frac{1}{2\cdot 2000}\\
&< 1
\end{aligned}$$

Thus, $0 < S-1001-1002-\cdots-2000 < 1$, implying that $S-1001-1002-\cdots-2000$ is not an integer, so is S. □

The second and last problem that we would like to present is the *Gaussian Moat problem* which is also related to the notions of primes in the ring of Gaussian integers, so we first define the following two objects.

Definition 4.2. *The set of Gaussian integers is defined as*

$$\mathbb{Z}[i] := \{a+bi, a,b\in\mathbb{Z}\}$$

which is a special case when $d=-1$ in Definition 2.5.

Then, the Gaussian primes are defined as follows.

Definition 4.3. *An element $a+bi\in\mathbb{Z}[i]$ is a Gaussian prime if it satisfies one of the following requirements up to associates:*
1) $a,b\neq 0$ and a^2+b^2 is a real prime,
2) $a=0$ and $|b|$ is an ordinary prime such that $b\equiv 3 \mod 4$,
3) $b=0$ and $|a|$ is an ordinary prime such that $a\equiv 3 \mod 4$.

Hence, the Gaussian Moat problem can be described as:

Problem 4.4. *The Gaussian moat problem asks whether it is possible to find an infinite sequence of distinct Gaussian prime numbers such that the difference between consecutive numbers in the sequence is bounded.*

The reason that we call this problem Gaussian "moat" is that we can think of ourselves stepping on the Gaussian primes in the complex plane. Then, if we want to prove that there is no such infinite sequence of distinct Gaussian prime numbers, we have to find an arbitrarily large moat bounding the point we start (See Figure 1.)

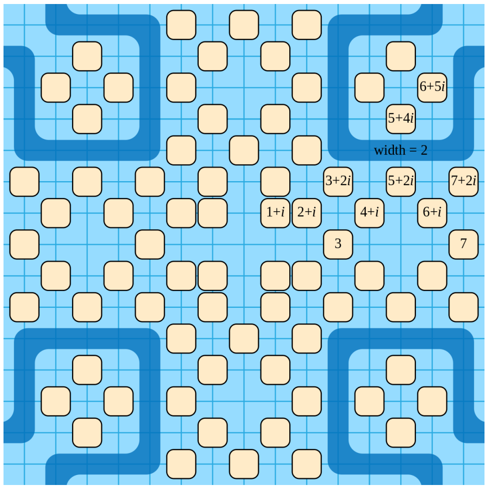

Figure 1. Gaussian Moat problem.

Mathematicians believe that there is no such infinite sequence, i.e., we can not walk to infinity with a bounded step size along the Gaussian primes. Interestingly, while the problem is still listed as an open problem, [D] claims that they have proved that it is indeed not possible but their paper has not been reviewed yet.

5. Conclusion

In this process of expanding my knowledge, I have learned the definitions of algebraic numbers and algebraic integers and their properties. It is intriguing how one could use the knowledge in this topic to solve a difficult-looking problem like 4.1 and how one could generate an interesting problem like 4.4. This topic involves several ideas discussed in class, namely, algebraic numbers and field extensions. I hope to continue working on this topic after the submission to explore more about primes in different rings of integers, which will help me get more insights into the project I have done regarding prime walks.

References

[CS] *Alg+NT=Algebraic Integers*, Cyclic Squares Channel, Retrieved from https://www.youtube.com/watch?v=ihw53v2ppIw.

[D] M. Das. *A Note on The Gaussian Moat Problem.* arXiv preprint arXiv:1908.10392 (2019).

[EWW] E. Gethner, S. Wagon, and B. Wick, *A Stroll Through the Gaussian Primes*, American Mathematical Monthly (1998).

[G] J. A. Gallian *Contemporary Abstract Algebra, 9th edition.* Cengage Learning, Boston MA, 2016.

[S] P. Samuel *Algebraic Theory of Numbers.* Academic Book Publisher, London, 1972.

[SL] *Quadratic Fields and Quadratic Number Rings.* Retrieved from https://studylib.net/doc/10744968/chapter-13-quadratic-fields-and-quadratic-number-rings-13.1.