Some notes on Algebraic Number Theory

These notes are my own approach to Algebraic Number Theory ("ANT"). I am covering one particular aspect which is whether or not unique factorisation applies in certain sets of complex numbers.

The approach is an attempt to be a mixture of formal and informal, and I have not followed the normal style of mathematical textbook or papers. Thus I am not terribly rigorous!

If you want more rigour, then I suggest that you have a look at some of the books suggested.

We are going to assume that you are familiar with what is traditionally called Elementary (or Classical Number) Theory ("ENT") which is the theory of the integers and includes many well-known results such as Fermat's Little Theorem and Fermat's Theorem on the sum of two squares. It is a very ancient branch of mathematics, and some of the results go back to Pythagoras and Euclid who lived over 2,500 years ago.

Algebraic Number Theory extends the ideas behind Elementary Number Theory to include properties of sets of numbers which behave in many ways like the integers. An example of such a set would be the Gaussian integers defined as $\mathbb{Z}[\sqrt{i}] = \{a + bi : a, b \in \mathbb{Z}\}$ where $i = \sqrt{-1}$. We shall see that these share lots of the properties of the integers (which we shall call from now on the 'rational integers') and we shall see how this specific example fits into a range of other sets of numbers which have very interesting properties.

Algebraic structures

One of the things that is often taken for granted in books on ENT is what is known as the algebraic structure of the integers. In essence this is that the sum, difference, and product of any two integers is itself an integer. We say that 'the integers are **closed** under the operations of addition, subtraction and multiplication' (but, of course, not division, since, for example $3 \div 4 \notin \mathbb{Z}$).

We can write this using the notation of set theory, where we use the symbol $\mathbb{Z}$ for the set of integers. We say that, $\text{for all } a, b \in \mathbb{Z},\ a + b \in \mathbb{Z},\ a - b \in \mathbb{Z} \text{ and } a \times b \in \mathbb{Z}$. The closure of the integers under subtraction implies that there is a special zero element, 0, which has the property that $\text{for all } a \in \mathbb{Z}, a + 0 = a$. We also have another special element, 1, which has the property that $a \times 1 = a$ for all $a \in \mathbb{Z}$.

A set of numbers that has the above properties is called a **ring**. In fact, a ring need not be solely composed of numbers, and we have been very informal about the definition. If you need a more complete definition, then have a look at, for example, https://kids.kiddle.co/Ring_(mathematics) .

Since we are dealing with rings of numbers there are certain properties that we can take for granted which do not necessarily apply if we are dealing with rings whose members are other sorts of objects. For example, multiplication is **commutative** which means that $a \times b = b \times a$ and there are no zero divisors, which means that, $\text{if } a \times b = 0 \text{ and } a \neq 0 \text{ then } b = 0$. With these two additional properties, a ring becomes an **integral domain** and all the sets of numbers we shall be investigating will be integral domains.

The Gaussian Integers

As I mentioned above, one of the first sets of numbers that was studied at what was the start of Algebraic number theory was that known as the Gaussian integers, named after their originator the famous mathematician Carl Friedrich Gauss.

We defined them in the introduction to this chapter, so I won't repeat the definition. The reason for the notation $\mathbb{Z}[i]$ will become apparent later. In fact, one textbook uses $\mathbb{Z} + i\mathbb{Z}$.

In this section we are going to see the properties they share with the rational integers and also those where they differ.

Algebraic structure

It is not particularly difficult to show that they are an integral domain. For example, consider closure under addition. Let $a, b, c, d \in \mathbb{Z}$ and thus $a + bi, c + di \in \mathbb{Z}[i]$. Then

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

Because the integers are closed under addition, $a + c \in \mathbb{Z}$ and $b + d \in \mathbb{Z}$ so

$$(a + c) + (b + d)i \in \mathbb{Z}[i]$$

Thus the Gaussian integers are closed under addition. The proofs that they are also closed under subtraction and multiplication are similar. It is obvious that $\mathbb{Z} \subset \mathbb{Z}[i]$.

Divisibility

The definition of divisibility in the rational integers is that we say that N is divisible by d (or d divides N), written as $d|N$, if there is an integer q such that $N = qd$. We use exactly the same definition for divisibility in the Gaussian Integers; just replace 'rational integer' by 'Gaussian integer' in the above definition.

It is fairly obvious that, because the rational integers are a subset of the Gaussian integers, if N and d happen to be rational integers then the same divisibility properties apply. Thus, very simply, $2 \,|6$ and $7 \,|56$. However, what if one or both of N and d are complex numbers? We find, for example, that