Boston University
Summer I 2008

MA341 Number Theory
Kalin Kostadinov

Lecture 8 (12 June 2008)

This Is Mostly About Rings

Introduction. We have seen in the lectures so far, for example while discussing Fermat's Last Theorem, or in the lecture about Quadratic Reciprocity Law, that questions about integers sometimes find their answers, or at least become more tractable, only when we go to a larger domains of numbers. The goal of this lecture is to define what these larger domains are somewhat more precisely, and to start the exploration of their properties.

The abstraction of the integers, a set with two operations satisfying some laws, gives birth to the concept of a *ring*. We will be intentionally vague about what exactly a ring is, and will we content ourselves with mentioning three very different examples: The set $\mathbb{C}$ of all complex numbers is a ring; the set $\mathbb{R}[x]$ of all polynomials of a single variable with real coefficients is a ring; the set $M_2(\mathbb{Z})$ of all two-by-two matrices with integer entries is a ring. In all three examples it is clear that what the addition and multiplication are, and that the sets are closed under this two operations.

We will concentrate on a particular kind of rings, to one that are of greatest interest in number theory. These are the so called *rings of algebraic integers*. One could form such a ring by starting with the set of integers, then throwing in some of the roots of a polynomial with integer coefficients and leading term 1, then adding all the possible linear combinations of the products of these roots, to guarantee that the set is closed under addition and multiplication.

This somewhat cumbersome recipe will be clarified by three very particular and important examples.

In each example, we will investigate how the properties of $\mathbb{Z}$ change. We will ask what are the primes numbers in the new ring, is there a unique factorization into primes, what is the analog of the Euler's ϕ-theorem, if any.

The Ring of Gaussian Integers. Our first example is the set all complex numbers with integral real and imaginary part:

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

This set is closed under addition, subtraction, and multiplication, so it is a subring of the ring of all complex numbers. It is obtained by the above recipe: start with $\mathbb{Z}$, through in a root of the equation $z^2 + 1 = 0$, say you call such a root i, then you throw in all its multiples, and then all the combinations $a + bi$, for arbitrary integers a, b.

Also notice that each element of GI is a root of polynomial with integer coefficients: $z = x + yi \in \mathbb{Z}[i]$, is root of $z^2 + 2xz + x^2 + y^2 = 0$.

When considering an element $z = x + yi \in \mathbb{Z}[i]$, it often helps to throw in the mix the element $\overline{z} = x - yi$, which is the other root of the equation for z, and we have the properties that both $z + \overline{z} = 2x$ and $z \cdot \overline{z} = x^2 + y^2$ are ordinary integers. The for an element $z \in \mathbb{Z}[i]$ the product $z\overline{z}$ is called the *norm* of z.

So the norm of an element in $\mathbb{Z}[i]$ is a non-negative ordinary integer, zero is the only element with a zero norm, and the norm of an ordinary integer is equal to its square. A big part of the usefulness of the norm stems from the fact that it is *multiplicative*

$$\begin{aligned}&\text{Norm}\left((a+bi)(c+di)\right) = \text{Norm}\left((ac-bd)+(ad+bc)i\right) = \\ &= (ac-bd)^2+(ad+bc)^2 = (a^2+b^2)(c^2+d^2) = \text{Norm}(a+bi)\text{Norm}(c+di)\end{aligned}$$

We mention without proof that the division algorithm property holds in $\mathbb{Z}[i]$, where for a measure of the smallness of the remainder we use the norm; this entails the existence of Euclidean algorithm, hence unique factorization in $\mathbb{Z}[i]$.
Which are the prime elements of $\mathbb{Z}[i]$? First notice that a prime element of $\mathbb{Z}[i]$ divides a unique prime of $\mathbb{Z}$. Indeed, if $z \in \mathbb{Z}[i]$ is prime, than z divides the ordinary integer $n = z \cdot \overline{z}$; if none of the ordinary prime factors of the number n was divisible by z, then n will have a factorization into primes in $\mathbb{Z}[i]$ not containing the prime z, which contradicts the uniqueness of the factorization in $\mathbb{Z}[i]$. Hence there exists an ordinary prime that is a multiple of z. There cannot be two such different primes, since two different primes are relatively prime in $\mathbb{Z}$, and hence relatively prime in $\mathbb{Z}[i]$, or in any larger domain containing $\mathbb{Z}$.
Therefore, to determine the primes of $\mathbb{Z}[i]$, it is enough to find out how the primes of $\mathbb{Z}$ factor in $\mathbb{Z}[i]$.
Surprisingly, this is determined by whether or not an ordinary prime is sum of two squares of ordinary integers.
Let $z = x + yi$ be a prime element of $\mathbb{Z}[i]$ which divides a prime $p \equiv 3 \pmod 4$. So $p = zw$, for some $w = u + iv \in \mathbb{Z}[i]$. Then
$p^2 = \text{Norm}(p) = Norm(zw) = (x^2+y^2)(u^2+v^2)$. This means that $u^2+v^2 = 1$ and $x^2+y^2 = p^2$, so that $z = \pm p$ or $z = \pm ip$, which means that primes $p \equiv 3 \pmod 4$ stay primes when considered as elements of $\mathbb{Z}[i]$.
Let now $p \equiv 1 \pmod 4$. Then there exists $x, y \in \mathbb{Z}$ such that $p = x^2 + y^2$, so that we could factor p as $p = (x+yi)(x-yi)$. Both $x+yi$ and $x-yi$ are primes in $\mathbb{Z}[i]$, as could be easily seen by another norm argument for example, and they are essentially different primes. The only other type of prime of $\mathbb{Z}[i]$ is represented by the element $1+i$, which is the divisor of the ordinary prime 2, as seen in $2 = -i(1+i)^2$.

A real quadratic ring.

A Cyclotomic Field.