Lecture 20

3.4 Euclidean domains, UFDs, the Gaussian integers

We have seen that if we take numbers of the form "$a+\alpha b$" for some α root of an irreducible polynomial and $a, b \in \mathbb{Q}$ (this needs to be made precise) we get a new field in which our polynomials is reducible. We have also seen that $\mathbb{C}$ is obtained in a similar manner from $\mathbb{R}$ by introducing the number i. What happens if we do something similar over $\mathbb{Z}$? We shall consider an important example which is also an example of various types of algebraic structures which generalise the ring of integers.

Definition (Gaussian integer) A Gaussian integer is a complex number $a+bi$ where $a, b \in \mathbb{Z}$.

The norm of a Gaussian integer $\alpha = a+bi$ is defined as $N(\alpha) = a^2+b^2$.

The set of Gaussian integers is denoted $\mathbb{Z}[i]$.

Example $\alpha = 1+i$ is a Gaussian integer. $N(\alpha) = 1^2+1^2 = 2$

As we may expect, the following holds.

Fact (*) $\mathbb{Z}[i]$ is an integral domain. (remember: a ring in which if $ab=0$ then $a=0$ or $b=0$)

This is clear if we think that $\mathbb{Z}[i] \subseteq \mathbb{C}$. However, it is interesting to show it by means of properties of the norm.

Properties of N For all $\alpha, \beta \in \mathbb{Z}[i]$:

- $N(\alpha) \geq 0$, with equality holding if and only if $\alpha = 0$
- $N(\alpha\beta) = N(\alpha)N(\beta)$

This tells us that if $\alpha\beta = 0$ then $N(\alpha\beta) = 0$

But $N(\alpha\beta) = N(\alpha)N(\beta)$ which is the product of two integers, which is 0 if and only if $N(\alpha) = 0$ or $N(\beta) = 0$, which by the properties of the norm means if $\alpha = 0$ or $\beta = 0$, showing (*) holds.

The norm on $\mathbb{Z}[i]$ turns out to satisfy some good properties which make a division algorithm possible in $\mathbb{Z}[i]$. Functions like these (in the case of $\mathbb{Z}$ we use the identity, in the case of rings of polynomials we use the degree) are called valuations and integral domains in which the division algorithm and Euclidean algorithm work are called Euclidean domains

As we said $N(\cdot)$ takes the role of deg in the division algorithm, so at every step we find a number of smaller norm as remainder (until we hit 0)

Example Let $\alpha = 1-8i$ and $\beta = 5+5i$ So $N(\alpha) = 1^2+8^2 = 65$ and $N(\beta) = 5^2+5^2 = 50$

Goal: write $\alpha = \beta \cdot \gamma + \delta$ where $N(\delta) < N(\beta)$

In this case we would have $1-8i = (-1-i)\cdot(5+5i) + (1+2i)$ (γ and δ)

Unlike $\mathbb{Z}$ and $F[x]$, here there's no "uniqueness" for the remainder & (and thus the quotient)

$N(1+2i) = 1+2^2 = 5 < N(\beta)$

(we won't show how this algorithm works in general)

The Gaussian integers also form a Unique factorisation domain (i.e. an integral domain in which a Unique factorisation thm holds).

What are the units of this ring? What the primes?

↑ recall: ring elements with a multiplicative inverse in the ring

It turns out that $\mathcal{U}(\mathbb{Z}[i]) = \{\alpha \in \mathbb{Z}[i] : N(\alpha) = 1\}$ which means $\mathcal{U}(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$

So the units of $\mathbb{Z}$ are also units in $\mathbb{Z}[i]$, with two additional elements.

Now, consider the "rational prime" 5. In $\mathbb{Z}[i]$ we have

$5 = (1+2i)(1-2i)$; as neither factor is a unit, this is a proper factorisation, so 5 is <u>not</u> irreducible in $\mathbb{Z}[i]$

What are the primes here?

If $N(\alpha) = p$ a rational prime, then by definition & properties of the norm, we get that α is an irreducible element of $\mathbb{Z}[i]$