Introduction to Number Theory-Tutorial 2

Sean Bray, Jason Coyle, Clara Kavanagh, Owen Ward, Olena Yavorska

February 2, 2014

1 Question 1

First deal with the case α is an algebraic integer. Deal with $b \neq 0$ first. $f(\alpha) = 0$
As $\mathbb{Z}[x]$ is a a UFD $\Rightarrow f(x) = u.p_1(x).....p_k(x)$ where all p_i are irreducible in $\mathbb{Z}[x]$ and u invertible element of $\mathbb{Z}[x]$ $\Rightarrow u$ an invertible element of $\mathbb{Z} \Rightarrow u = \pm 1$.
As $f(x) = \sum\limits_{1=0}^{n} f_i x^i$ with $f_n = 1 \Rightarrow \forall p_i$ we have leading coefficient =1 As $f(\alpha) = 0 \ \Rightarrow \exists p_i \in \mathbb{Z}[x] = p$ s.t $p(\alpha) = 0$
As p is irreducible $\Rightarrow$ $p(x)$ is the minimal polynomial of in $\mathbb{Z}[x]$. $\Rightarrow$ p is irreducible in $\mathbb{Z}[x]$ and it follows from Gauss's lemma p irreducible in $\mathbb{Q}[x]$.
$\Rightarrow p(x)$ is the minimal polynomial of α in $\mathbb{Q}[x]$.
From MA2215, we have $[\mathbb{Q}[\alpha] : \mathbb{Q}] = deg(p) \Rightarrow$ Basis of $\mathbb{Q}[\alpha]$ over $\mathbb{Q}$ is 1,$\sqrt{D}$
$\Rightarrow [\mathbb{Q}[\alpha] : \mathbb{Q}] = Dim\mathbb{Q}[\alpha] = 2 = deg(p)$ $p(x) = x^2 + p_1 x + p_0, p_1, p_0 \in \mathbb{Z}$ Using quadratic formula,
$\alpha = a + b\sqrt{D} = \frac{-p_1}{2} \pm \frac{\sqrt{p_1^2 - 4p_0}}{2}$ $a = \frac{-p_1}{2} 2a = -p_1 \in \mathbb{Z} \Rightarrow \ \alpha + \overline{\alpha} \in \mathbb{Z}$
$b\sqrt{D} = \frac{\sqrt{4a^2 - 4p_0}}{2}$, $b^2 D = \frac{(4a^2 - 4p_0)}{4} = a^2 - p_0$ $a^2 - b^2 D = P_0$ But $a^2 - b^2 D = \alpha\overline{\alpha}$
$\Rightarrow \alpha\overline{\alpha} = P_0 \in \mathbb{Z}$
True for $b \neq 0$.
For $b = 0$
$b = 0 \Rightarrow deg(P) = [\mathbb{Q}[\alpha] : \mathbb{Q}] = 1 \Rightarrow p(x) = x + p_0 \ \Rightarrow p(\alpha) = \alpha + p_0 = 0 \ \Rightarrow$ $+ p_0 = 0 \Rightarrow \alpha = -p_0 \in \mathbb{Z}$ so true for $b = 0$
For other direction assume $\alpha + \overline{\alpha} = m \in \mathbb{Z}$, $\alpha\overline{\alpha} = n \in \mathbb{Z}$
$\Rightarrow \alpha + \overline{\alpha} - m = 0 \Rightarrow \alpha(\alpha + \overline{\alpha} - m) = 0$
$\Rightarrow \alpha^2 - \alpha\overline{\alpha} - \alpha = 0 \Rightarrow \alpha^2 - m\alpha + n = 0$
Let$f(x) = x^2 - mx + n \in \mathbb{Z}[x] \Rightarrow f(\alpha) = 0 \Rightarrow \alpha$ is an algebraic integer

2 Question 2

We shall let

$$\omega = \begin{cases} \frac{1+\sqrt{D}}{2} & D \equiv 1 \ (mod\ 4) \\ \sqrt{D} & D \equiv 2,3 \ (mod\ 4) \end{cases}$$

so that the result proved above means that we have $O_{\sqrt{D}} = \mathbb{Z} \bigoplus \mathbb{Z}\omega$

$$\alpha = a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$$

$$\alpha + \bar{\alpha} = 2a \in \mathbb{Z}$$

$$N(\alpha) = \alpha\bar{\alpha} = a^2 - Db^2 \in \mathbb{Z}$$

So $2a \in \mathbb{Z} \Rightarrow a \in \mathbb{Z}$ OR $a \in 1/2 + \mathbb{Z}$
If $a \in \mathbb{Z}$ and $a^2 - Db^2 \in \mathbb{Z}, Db^2 \in \mathbb{Z}$

$$\Rightarrow b = \frac{c}{d} \qquad gcd(c,d) = 1$$

$$\frac{Dc^2}{d^2} \in \mathbb{Z} \Rightarrow \frac{d^2}{D} \text{ D is square free}$$

$$\Rightarrow d^2 = 1$$

$$\Rightarrow d = \pm 1 \text{ and } b \in \mathbb{Z}$$

If $a = n + 1/2 \in 1/2 + \mathbb{Z}$

$$a^2 = n^2 + n + \frac{1}{4}$$

$$a^2 - Db^2 = M$$

Therefore $Db^2 = K + \frac{1}{4} \quad b = \frac{c}{d} \quad gcd(c,d) = 1$

$$\frac{Dc^2}{d^2} = \frac{4K+1}{4} \Rightarrow Dc^2 = (4K+1)d^2$$

$$\Rightarrow \frac{4}{d^2} \Rightarrow d^2 = 4 \Rightarrow d = 2l$$

$$4Dc^2 = 4l^2(4K+1) \;\Rightarrow\; \frac{Dc^2}{l^2} = 4K+1$$

$$gcd(c,l) = 1 \Rightarrow \frac{l^2}{D} \;\Rightarrow l^2 = 1$$

$$b = \frac{c}{d} = \frac{c}{2} \in \frac{1}{2} + \mathbb{Z} \text{ (c,d are of the same type)}$$

$$a^2 - Db^2 \in \mathbb{Z} \text{ iff } D \equiv x \text{ (mod4)}, D = 4m + x$$

$$a^2 - 4mb^2 - ab^2 \in \mathbb{Z}$$

If $x = 2$ or 3 and $a = n + \frac{1}{2} \qquad b = S + \frac{1}{2} \;\; N + \frac{1}{4} + M - xS = \frac{x}{4}$ If $x = 2, 3$ $(D \equiv 2, 3)$ then this cannot be in $\mathbb{Z}$ so $a, b \in \mathbb{Z}$

3 Question 3

Let α be invertible $\Rightarrow \;\exists\beta$ such that $\alpha\beta = 1$
$\Rightarrow N(\alpha\beta) = N(\alpha)N(\beta) = 1 \;\Rightarrow\; N(\alpha) = 1$
Let $\alpha = a + b\sqrt{D} \;\Rightarrow\; N(\alpha) = a^2 - b^2D$. As $a^2 \geq 0,\ b^2 \geq 0,\ -D > 0$ we have that $N(\alpha) \geq 0 \Rightarrow\; N(\alpha) = 1, \;\Rightarrow\; a^2 - b^2D = 1$. If $a^2 \geq 1 \;\Rightarrow\; 1 = a^2 - b^2D \geq 1 - b^2D \;\Rightarrow b = 0$ so $a = \pm 1$.
If $a = 0, \;\Rightarrow\; -b^2D = 1$ but if $b \geq 2$ this gives a contradiction.

- If $b = \pm\frac{3}{2},\ D = \frac{-4}{9} \notin \mathbb{Z}$
- If $b = \pm 1,\ D = -1$ and so $\sqrt{-1}$ is invertible with inverse $-\sqrt{-1}$
- If $b = \pm\frac{1}{2},\ D = -4$ which is not relevant as D is not square free

If $a = \pm\frac{1}{2}, \Rightarrow \; -b^2D = \frac{3}{4} \Rightarrow \; b^2 \leq \frac{3}{4}$ as $-D \geq 1 \Rightarrow b^2 = \frac{1}{4} \;\; \Rightarrow \;\; b = \pm\frac{1}{2}$ so $D = -3$
Also, $\pm\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$ is invertible with conjugate inverse.
So, all invertible elements are:

- $(\pm 1, \; \pm\sqrt{-1}) \in O_{\sqrt{-1}}$
- $(\pm 1, \; \pm\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}) \in O_{\sqrt{-3}}$
- $(\pm 1) \in O_{\sqrt{D}}$ where $D \neq -1, -3$

4 Question 4

We consider two cases here,
Case 1: where $D = -1, -2$
Then, for $\omega = \sqrt{D}$ the parallelogram is shown below, which has sides of length 1 and $\sqrt{|D|}$. It is clear the centre a, the intersection of the diagonals, is the furthest point away from the vertices. By Pythagoras, the distance from the centre to a vertex (Y) is:

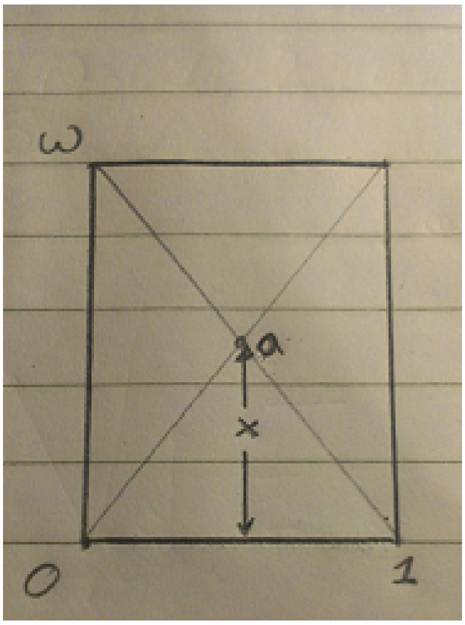

Figure 1: Parallelogram for Case 1

$$Y^2 = \left(\frac{1}{2}\right)^2 + X^2 = \left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{-D}}{2}\right)^2 = \frac{1-D}{4}$$

which is < 1 for $D = -1, -2$ so the result follows.
Case 2: where $D = -3, -7, -11$
Then $\omega = \frac{1+\sqrt{D}}{2}$ and the parallelogram is shown below.
This can be broken into two isosceles triangles, as seen above, which will have

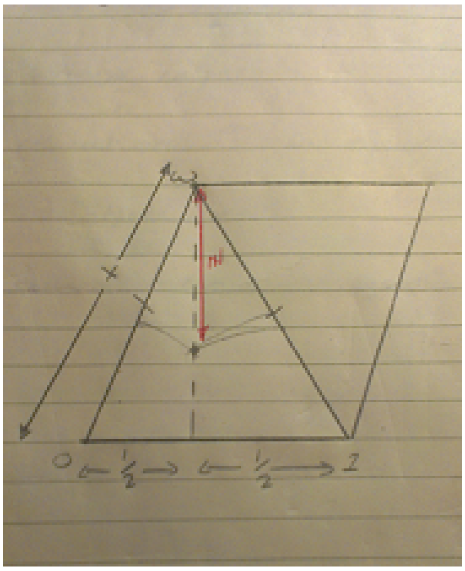

Figure 2: Parallelogram for Case 2

height $\frac{\sqrt{-D}}{2}$ and side lengths $\sqrt{\frac{1-D}{4}}$ and 1. Then, if we swing arcs of radius 1 from each of the bottom two vertices, it is clear that any point in the triangle within these arcs is a distance less than 1 from a vertex. The only point that remains to be checked is where these arcs cross, located on the line joining the midpoint of the base and the top vertex. Calling the distance of this point from the top vertex z we must show that $z < 1$ for $D = -3, -7, -11$
Using Pythagoras, we get $z = \frac{\sqrt{-D}}{2} - \frac{\sqrt{3}}{2}$. If this is < 1 then

$$z = \frac{\sqrt{-D}}{2} - \frac{\sqrt{3}}{2} < 1$$
$$\Rightarrow \ -D - 1 < 2\sqrt{-3D}$$

and squaring this

$$\Rightarrow \ D^2 + 2D + 1 < -12D$$

which is true for $D = -3, -7, -11$ so $|z| < 1$ as required.

5 Question 5

By the previous question,any point in the parallelogram, $z, z+\beta, z+\beta\omega, z+\beta(\omega+1)$ is a distance at most β from one of the vertices. So any point in the lattice $\mathbb{Z} \oplus \omega\mathbb{Z}$ ia at distance at most β from a point in the lattice $\mathbb{Z} \oplus \omega\beta\mathbb{Z}$ because the lattice divides $\mathbb{C}$ into such parallelograms.
$\Rightarrow \ \forall \ \alpha \in O_{\sqrt{D}} \ \exists\gamma, \ \delta$ such that $\alpha = \gamma\beta + \delta$ with $\gamma\beta$ the nearest point in the lattice, and so,

$$N(\delta) = N(\alpha - \gamma\beta) = \text{ Distance Squared } < \beta^2$$
$$\Rightarrow \ N(\delta) < \beta^2 = N(\beta)$$

This holds for all $\beta \neq 0$ $\beta \in O_{\sqrt{D}}$ and so $O_{\sqrt{D}}$ is norm-Euclidean.