Algebraic Number Theory - Assignment 1

Matteo Durante, 2303760, Leiden University

18th September 2018

Exercise 8

Let's define the norm on $\mathbb{Z}[\sqrt{3}]$ to be $N(a+b\sqrt{3}) = |a^2 - 3b^2|$.

We notice that

$$\begin{aligned} N((a+b\sqrt{3})(c+d\sqrt{3})) &= N((ac+3bd)+(ad+bc)\sqrt{3}) \\ &= |((ac+3bd)-(ad+bc)\sqrt{3})((ac+3bd)+(ad+bc)\sqrt{3})| \\ &= |(a-b\sqrt{3})(c-d\sqrt{3})(a+b\sqrt{3})(c+d\sqrt{3})| \\ &= N(a+b\sqrt{3})N(c+d\sqrt{3}), \end{aligned}$$

i.e. it preserves the products.

Let $a, b \in \mathbb{Z}[\sqrt{3}]$ with $b \neq 0$ and suppose $a = c + d\sqrt{3}$, $b = e + f\sqrt{3}$.

We can see that

$$\begin{aligned} \frac{a}{b} &= \frac{c+d\sqrt{3}}{e+f\sqrt{3}} \frac{e-f\sqrt{3}}{e-f\sqrt{3}} \\ &= \frac{ce-3df}{e^2-3f^2} + \frac{-cf+de}{e^2-3f^2}\sqrt{3} \\ &= p + q\sqrt{3} \end{aligned}$$

where $p = \dfrac{ce-3df}{e^2-3f^2}$ and $q = \dfrac{-cf+de}{e^2-3f^2}$.

Let n be the closest integer to p and let m be the closest integer to q (if there is an ambiguity in the choice, pick any of them). Notice that $|n-p| \leq 1/2$ and $|m-q| \leq 1/2$.

We want to show that $a = (n+m\sqrt{3})b + \gamma$ for some $\gamma \in \mathbb{Z}[\sqrt{3}]$ such that either $\gamma = 0$ or $N(\gamma) < N(b)$.

Define $\theta := (n-p) + (m-q)\sqrt{3}$ and let $\gamma = b\theta \in \mathbb{Z}[\sqrt{3}]$; now, notice that

$$\begin{aligned} \gamma &= b\theta \\ &= b((n-p)+(m-q)\sqrt{3}) \\ &= b(n+m\sqrt{3}) - b(p+q\sqrt{3}) \\ &= b(n+m\sqrt{3}) - b\frac{a}{b} \\ &= b(n+m\sqrt{3}) - a \end{aligned}$$

From this, we get $a = b(n + m\sqrt{3}) + \gamma$.

Observing that

$$\begin{aligned} N(\gamma) &= N(b\theta) \\ &= N(b)N(\theta) \\ &= N(b)|(n-p)^2 - 3(m-q)^2| \\ &\le N(b)\max\{(n-p)^2, 3(m-q)^2\} \\ &=\le \frac{3}{4}N(b) \\ &< N(b) \end{aligned}$$

we can finally conclude that $\mathbb{Z}[\sqrt{3}]$ is an Euclidean Domain, and therefore a Principal Ideal Domain.

Exercise 17

Let $\alpha = a + bi$ and consider the chain of ideals $(a^2 + b^2) \subset (a + bi) \subset \mathbb{Z}[i]$.

For any positive integer n, we get that $[Z[i] : (n)] = n^2$ because $\mathbb{Z}[i]/(n) \cong \mathbb{Z}[x]/(x^2 + 1, n) \cong (\mathbb{Z}/n\mathbb{Z})[x]/(x^2 + 1)$ (by [1, chap. 7, thm 8(2)] and [1, chap. 9, prop. 2]), whose elements are the classes of the following ones $\{a + bx \mid a, b \in \mathbb{Z}/n\mathbb{Z}\}$ since they can be represented by polinomials of degree < 2 and with natural coefficients lower than n; furthermore, the classes of the elements of the set are all distinct.

Thus, $[Z[i] : (a^2 + b^2)] = (a^2 + b^2)^2 = N(\alpha)^2$.

As an additive group, $[\mathbb{Z}[i] : (a^2 + b^2)] = [\mathbb{Z}[i] : (a + bi)][(a + bi) : (a^2 + b^2)]$.

As a quotient group, $\mathbb{Z}[i]/(a - bi) \cong (a + bi)/(a^2 + b^2)$ (we can see this by sending $x + yi$ to $(x + yi)(a + bi)$).

Noticing that $\mathbb{Z}[i]/(a + bi) \cong \mathbb{Z}[i]/(a - bi)$ as additive groups by using complex conjugation, we get that $N(\alpha) = [\mathbb{Z}[i] : (a + bi)] = |\mathbb{Z}[i]/(a + bi)|$, as stated.

References

[1] D.S. Dummit, R.M. Foote, *Abstract Algebra*, Whiley, Third edition, 2003.