UNIQUE FACTORISATION AND QUADRATIC FIELDS (MA2316, SECOND WEEK)

VLADIMIR DOTSENKO

Our goal for now will be to have a summary of known results about unique and non-unique factorisation in number-theoretic rings. The plethora of available results is really impossible to cover in full, so for the purpose of this introductory course we shall discuss integers in quadratic number fields. More precisely, for each D that is not a perfect square, one can form the quadratic number field $\mathbb{Q}(\sqrt{D})$, the field extension of $\mathbb{Q}$ inside $\mathbb{C}$ consisting of all complex numbers $\alpha = a + b\sqrt{D}$ where $a, b \in \mathbb{Q}$. To understand the structure of that field, we may assume without loss of generality that D is square-free, and we shall assume this implicitly throughout this note. The ring $\mathcal{O}_{\sqrt{D}}$, called the *ring of integers* in $\mathbb{Q}(\sqrt{D})$ consists of all elements $\alpha \in \mathbb{Q}(\sqrt{D})$ for which there exists a polynomial $f(x) \in \mathbb{Z}[x]$ with leading coefficient 1 such that $f(\alpha) = 0$.

Fact. The ring $\mathcal{O}_{\sqrt{D}}$ consists of all complex numbers $\alpha = a + b\sqrt{D}$ with $a, b \in \mathbb{Z}$ if $D \equiv 2, 3 \pmod 4$, and consists of all complex numbers $\alpha = a + b\sqrt{D}$ with $a, b \in \mathbb{Z}$ or $a, b \in \frac{1}{2} + \mathbb{Z}$ if $D \equiv 1 \pmod 4$. In the latter case, it can be described alternatively as all complex numbers $\alpha = a + b\frac{1+\sqrt{D}}{2}$ with $a, b \in \mathbb{Z}$.

We shall let

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

so that we have

$$\mathcal{O}_{\sqrt{D}} = \mathbb{Z} \oplus \mathbb{Z}\omega.$$

For that (and further on), we shall use extensively the *norm* function $N(a+b\sqrt{-D}) = |a^2 - b^2D|$. For $D < 0$ (imaginary quadratic fields), this function is the square of the complex absolute value; as such it satisfies $N(\alpha\beta) = N(\alpha)N(\beta)$. In fact, this equation is satisfied for $D > 0$ (real quadratic fields) as well. We note that this function assumes integer values even for $D \equiv 1 \pmod 4$ and $a, b \in \frac{1}{2} + \mathbb{Z}$.

As a warming up example, let us prove the following result.

Theorem 1. *The ring $\mathcal{O}_{\sqrt{-5}}$ is not a UFD.*

Proof. Let us examine the decompositions $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. We have $N(2) = 4$, $N(3) = 9$, $N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$. We shall show that all these four elements are prime (irreducible) elements of $\mathcal{O}_{\sqrt{-5}}$. Suppose, for instance, that $2 = \gamma\delta$, where γ and δ are not invertible. Then $4 = N(2) = N(\gamma)N(\delta)$, so either one of the norms is equal to 1, or we have $N(\gamma) = N(\delta) = 2$. The latter is impossible since the equation $a^2 + 5b^2 = 2$ has no integer solutions. In the former case, without loss of generality $N(\gamma) = 1$, but the only integer solutions to the equation $a^2 + 5b^2 = 1$ are $a = \pm 1$, $b = 0$, corresponding to invertible elements $\pm 1 \in \mathcal{O}_{\sqrt{-5}}$. The same reasoning applies in all other cases, where in addition one checks that there are no elements of norm 3 in $\mathcal{O}_{\sqrt{-5}}$. □

We shall see below that describing invertible elements, as well as elements of norm 2 and 3 in imaginary quadratic fields will be of certain importance.

Recall that the easiest way to prove that a ring is a UFD (unique factorisation domain) is to prove that it is a Euclidean domain. A domain R is *Euclidean* if it is equipped with a function $\|\cdot\|\colon R\setminus\{0\}\to\mathbb{N}$ for which (1) $\|\alpha\|\ge\|\beta\|$ whenever α is divisible by β, and (2) for each α and each $\beta\ne 0$, there exist $\gamma,\delta\in R$ such that $\alpha=\beta\gamma+\delta$, and $\delta=0$ or $\|\delta\|<\|\beta\|$. In a Euclidean domain, every ideal is principal, which in turn implies the uniqueness of factorisation into primes. (For details, check your notes for the 2215 module.)

The ring $\mathcal{O}_{\sqrt{D}}$ is said to be *norm-Euclidean* if it is Euclidean for $\|\beta\|=N(\beta)$.

Theorem 2. *The ring $\mathcal{O}_{\sqrt{D}}$ is Euclidean if and only if it is norm-Euclidean. This happens precisely for $D=-1,-2,-3,-7,-11$.*

Proof. Let us first show that for D not on the list above, the ring $\mathcal{O}_{\sqrt{D}}$ is not Euclidean. The proof consists of some routine work, and the following clever step.

Lemma. *If $\mathcal{O}_{\sqrt{D}}$ is Euclidean and has exactly k invertible elements, then there exists a non-invertible element $\beta\in\mathcal{O}_{\sqrt{D}}$ with $N(\beta)\le k+1$.*

Proof. Let us take for β one of the non-invertible elements of $\mathcal{O}_{\sqrt{D}}$ with the least possible $\|\beta\|$. Then for each element α, there exist $\gamma,\delta\in\mathcal{O}_{\sqrt{D}}$ such that $\alpha=\beta\gamma+\delta$, and $\delta=0$ or $\|\delta\|<\|\beta\|$. This shows that δ is either 0 or invertible. Therefore, the number of elements of the quotient ring $\mathcal{O}_{\sqrt{D}}/(\beta)$ is at most $k+1$.

It remains to recall (or notice) that the number of elements of the quotient ring $\mathcal{O}_{\sqrt{D}}/(\beta)$ is equal to $N(\beta)$. The easiest way to see it is geometric: the ideal generated by $\beta=a+b\omega$ in $\mathcal{O}_{\sqrt{D}}$ is freely spanned over integers by β and $\omega\beta$. The 2D vectors corresponding to these vectors form a parallelogram whose area relative to the area of the parallelogram formed by the vectors representing 1 and ω is $N(\beta)$. That easily implies that the former parallelogram contains $N(\beta)$ points of the form $c+d\omega$ with integer c and d, which are precisely representatives of cosets in the quotient ring $\mathcal{O}_{\sqrt{D}}/(\beta)$. □

It is easy to check that for D not on the list above the only invertible elements in $\mathcal{O}_{\sqrt{D}}$ are ±1. (Indeed, we instantly see that $N(x)=1$ for an invertible x, and that reduces the question to routinely checking finitely many cases). Therefore, we can prove the result by contradiction using the following simple observation.

Lemma. *For $D\ne-1,-2,-3,-7,-11$, the only elements $\beta\in\mathcal{O}_{\sqrt{D}}$ with $N(\beta)\le 3$ in are $\beta=\pm1$.*

Proof. The proof is completely routine. For $D\equiv 2,3 \pmod 4$ we have $D\le-5$, and $N(a+b\sqrt{D})=a^2-Db^2\ge 4$ for $a,b\in\mathbb{Z}$ unless $a=\pm1$, $b=0$. For $D\equiv 1 \pmod 4$ we have $D\le-15$, so $N(a+b\sqrt{D})=a^2-Db^2\ge 4$ for $a,b\in\mathbb{Z}$ or $a,b\in\frac{1}{2}+\mathbb{Z}$ unless $a=\pm1$, $b=0$. □

The remaining part, that is the claim that for D on the list above, the ring $\mathcal{O}_{\sqrt{D}}$ is norm-Euclidean, will be justified in the next tutorial. □

Remark. *There exist non-Euclidean rings of integers in imaginary quadratic fields that are UFD, these are precisely $\mathcal{O}_{\sqrt{D}}$ for $D=-19,-43,-67,-163$. (Baker–Stark, 1966).*

For $D>0$, the situation changes dramatically. First of all, there are more norm-Euclidean rings: those are precisely $\mathcal{O}_{\sqrt{D}}$ for $D=2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73$. Because this list is quite long, it took more than 100 years (1848–1952) and a few dozens of mathematicians to complete the proof. (The first step, done by Wantzel, who proved that for $D=2,3,5$ the ring $\mathcal{O}_{\sqrt{D}}$ is norm-Euclidean, the last step by Barnes and Swinnerton–Dyer, who proved that for $D=97$ the ring $\mathcal{O}_{\sqrt{D}}$ is not norm-Euclidean. More strikingly, for $D>0$ among the rings $\mathcal{O}_{\sqrt{D}}$ there exist

Euclidean rings which are not norm-Euclidean. The smallest example of such is $\mathcal{O}_{\sqrt{14}}$, which was only proved by Harper in 2000, after a long period of resistance to many different approaches. An older and more elementary example is that of Clark (1994) who proved that $\mathcal{O}_{\sqrt{69}}$ is Euclidean but not norm-Euclidean. These results, however, are less surprising than they may appear at a first glance: it has been known for a long time that both $\mathcal{O}_{\sqrt{14}}$ and $\mathcal{O}_{\sqrt{69}}$ are UFDs, and it is also known (Weinberger, 1973) that assuming "generalised Riemann hypotheses" the UFD property implies that the ring is Euclidean for a very large class of rings of algebraic integers including $\mathcal{O}_{\sqrt{D}}$ with $D > 0$. Most recently, Narkiewicz (2007) proved that among the rings $\mathcal{O}_{\sqrt{D}}$ with $D > 0$ that are UFDs there exist at most two which are not Euclidean.