AN ELEMENTARY PROOF THAT NOT ALL PRINCIPAL IDEAL DOMAINS ARE EUCLIDEAN DOMAINS

ROBERT A. WILSON

1. Introduction

A standard result in undergraduate algebra courses is that every Euclidean domain (ED) is a principal ideal domain (PID). It is routinely stated, but rarely proved, that the converse is false. The ring $R = \mathbb{Z}[\theta]$, where $\theta = (1+\sqrt{-19})/2$, so that $\theta^2 = \theta - 5$, is sometimes mentioned as a counterexample. The proof that R is indeed a counterexample is due to Motzkin [1] in 1948, as a special case of much more general results. A more elementary proof, accessible to advanced undergraduates, is given by Cámpoli [2] in 1988, though with a more restricted definition of Euclidean norm than Motzkin uses.

The first part of this proof, that R is not a Euclidean domain, Cámpoli attributes to the referee of his paper. It is worth remarking, however, that that proof, with very little modification, actually proves Motzkin's slightly more general result, namely that R is not a Euclidean domain under the following definition.

Definition 1. *A Euclidean function on an integral domain A is a function $d : A \setminus \{0\} \to \mathbb{N} \cup \{0\}$ with the property that, for all $a, b \in A$, with $b \neq 0$, there exist $q, r \in A$ such that $a = bq + r$ and either $d(r) < d(b)$ or $r = 0$. In this situation, A is called a Euclidean domain.*

Notice this does not include the property, usually included in the definition of Euclidean function, that if $a|b$ then $d(a) \leq d(b)$.

At the same time, it is possible to simplify the second part of Cámpoli's proof, that R is a PID, reducing his seven (or nine, depending on how you count them) cases to three (or four). This simplification comes from treating the problem as a geometric problem in the Argand diagram, rather than an arithmetic problem in the divisors of the coefficients x, y of elements $x + y\theta$ of R.

2. Basic properties of R

As above, let $\theta = (1+\sqrt{-19})/2$, and $R = \mathbb{Z}[\theta]$. Since $\theta^2 = \theta - 5$, we have that $R = \{a + b\theta \mid a, b \in \mathbb{Z}\}$. Since it is a subring of the complex numbers, it is an integral domain, that is, a commutative ring in which $\alpha\beta = 0$ implies $\alpha = 0$ or $\beta = 0$. Since $\bar{\theta} = 1 - \theta$, the ring R is invariant under complex conjugation. The ring R inherits from $\mathbb{C}$ the norm $N(\alpha) = \alpha\bar{\alpha} = |\alpha|^2$, which is multiplicative in the sense that $N(\alpha\beta) = N(\alpha)N(\beta)$.

Next we show that the only units (that is, divisors of 1) in R are $1, -1$. For if $a + b\theta$ (with $a, b \in \mathbb{Z}$) is a divisor of 1 in R, then $N(a + b\theta) = (a + b\theta)(a + b\bar{\theta})$ is a

Date: 11th November 2015; revised 19th January and 1st September 2016.

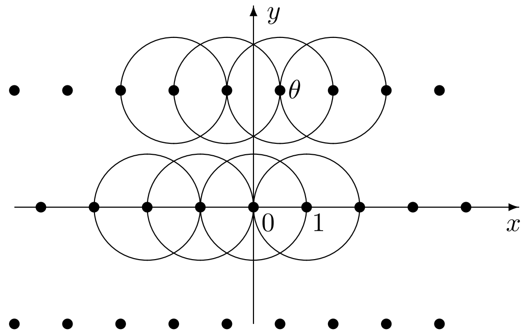

FIGURE 1. The proof that N is not a Euclidean function for R

divisor of 1 in $\mathbb{Z}$. Since $(a+b\theta)(a+b\bar{\theta}) = a^2+ab+5b^2 = (a+\frac{1}{2}b)^2+\frac{19}{4}b^2$, this implies that $b=0$, and therefore $a=\pm 1$.

A similar argument shows that the elements $2,3$ are irreducible in R, that is, their only factors are unit multiples of themselves and 1. For, if $a+b\theta$ is a proper divisor of 2 or 3 in R, then $(a+\frac{1}{2}b)^2+\frac{19}{4}b^2$ is a proper divisor of 4 or 9 in $\mathbb{Z}$, so is equal to 2 or 3. But then $b=0$ so $a^2=2$ or 3, which is impossible.

3. R is not a Euclidean domain

It is easy to see that N is not a Euclidean function for R. Motzkin [1] attributes this observation to Dedekind in 1894, but the reference is missing from [1]. We give a proof here, as it will provide useful context for the proof below that R is a principal ideal domain. The property that $a=bq+r$ with either $N(r)<N(b)$ or $r=0$ translates to saying that $|a/b-q|<1$, that is, every fraction a/b is at a distance strictly less than 1 from some element q of the ring. In Figure 1 we have drawn some circles of radius 1 centred on the elements of R to show that they do not cover the whole plane. Algebraically, we see that, for example, if $a=\sqrt{-19}$ and $b=4$, then a/b has distance $\sqrt{19}/4>1$ from the nearest lattice point.

It is slightly more difficult to show that there is *no* Euclidean function at all on R. In fact Motzkin proves that $\mathbb{Z}[(1+\sqrt{1-4n})/2]$ is not a Euclidean domain for any $n\geq 5$. The proof we now give also generalises easily to this situation.

Theorem 1. *The ring $R=\mathbb{Z}[\theta]$, where $\theta = 1+\sqrt{-19})/2$, is not a Euclidean domain.*

Proof. Assume that d is any Euclidean function on R. Choose $m\in A\setminus\{0,\pm 1\}$ with $d(m)$ as small as possible. Then there exist $q,r\in A$ such that $2=mq+r$, with either $d(r)<d(m)$ or $r=0$. The minimality of $d(m)$ implies $r=0,1,-1$. Hence $mq=2,1,3$. Then irreducibility of $2,3$ implies that $m=\pm 2,\pm 3$.

Similarly, there exist $q',r'\in A$ such that $\theta=mq'+r'$, with either $d(r')<d(m)$ or $r'=0$. Again, it follows that $r'=0,1,-1$, and therefore $mq'=\theta,\theta-1,\theta+1$. Now it is easy to see that none of $\theta,\theta\pm 1$ is divisible by 2 or 3, so this is a contradiction. □

4. Quasi-Euclidean domains

The proof given below that R is a PID is a slight generalisation of one of the standard proofs that every Euclidean domain is a PID. Recall that an ideal I of a commutative ring A is a nonempty subset with the property that for every $a,b\in I$

and $r \in A$, both $a - b$ and ar lie in I. The set bA of all multiples of b is easily seen to be an ideal, and is called the principal ideal generated by b. If every ideal is principal, then A is called a principal ideal domain.

Given any non-zero ideal I in a Euclidean domain A, we must find an element $b \in I$ such that $I = bA$. So, pick $b \in I$ such that $b \neq 0$ and $d(b)$ is as small as possible, and assume, for a contradiction, that $a \in I \setminus bA$. Then by the Euclidean property, there exist $q, r \in A$ with $r = a - bq \in I$ and either $d(r) < d(b)$ or $r = 0$. The former contradicts the minimality of $d(b)$, while the latter contradicts the assumption that a is not in bA.

Notice that the argument *almost* works more generally if we allow $r = ap - bq$ and not insisting that $p = 1$. However, if $p \neq 1$ then the case when $r = 0$ does not immediately lead to a contradiction, and an alternative argument is required. Our method is to exclude the case $r = 0$ completely, except in the case $p = 1$, when we cannot avoid it.

This suggests the following definition of a quasi-Euclidean domain (QED). (Note that this is not a standard definition, and there are other definitions of quasi-Euclidean domains in the literature, not necessarily equivalent to this one.)

Definition 2. *A quasi-Euclidean function (or Motzkin function) on an integral domain A is a function $d : A \setminus \{0\} \to \mathbb{N} \cup \{0\}$ with the property that, for all $a, b \in A$, with $b \neq 0$, there exist $p, q, r \in A$, with $p \neq 0$, such that $ap = bq + r$ and either*

- *$d(r) < d(b)$; or*
- *$p = 1$ and $r = 0$.*

In this situation, A is called a quasi-Euclidean domain (or Motzkin domain).

The above proof then generalizes immediately to a proof that every QED is a PID. However, it is not obvious that we have gained anything, as it is not obvious that there exist quasi-Euclidean domains that are not Euclidean. We shall resolve this by showing that R is indeed a QED.

5. R is a principal ideal domain

In the light of the previous section, it suffices to show that R is a QED in the sense defined above. Working in the field of fractions $\mathbb{Q}(\sqrt{-19})$, we can divide by b, and use the fact that $N(a)/N(b) = |a/b|^2$, so that the property $d(r) < d(b)$ translates to

$$0 < \left|\frac{a}{b}p - q\right| < 1.$$

After some initial reductions, the proof divides into three cases, in which we shall take $p = 1$, $p = 2$, and $p = \theta$ or $\bar{\theta}$ respectively. Figure 2 illustrates these three cases. The large dots represent the elements of R in the Argand diagram. The interiors (excluding the centres) of the large circles represent points a/b with $0 < |a/b - q| < 1$, for some $q \in R$, and the small circles similarly represent points with $0 < |2a/b - q| < 1$, or equivalently $0 < |a/b - q/2| < 1/2$. The small dots represent all the remaining values of a/b, that is $a/b = q/2$. The horizontal line represents points with imaginary part $\sqrt{3}/2$, which we may take as the boundary betweeen the cases $p = 1$ and $p = 2$.

The picture tells us what we have to do, and it only remains to fill in the algebraic details. The required result is the following.

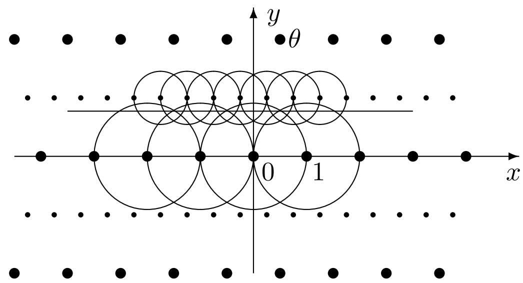

Figure 2. A graphical illustration of the proof that R is a PID

Lemma 1. *For every $a, b \in R$, with $b \neq 0$, and b not an exact divisor of a, there exist $p, q \in R$ such that*

$$0 < \left|\frac{a}{b}p - q\right| < 1.$$

Proof. Since we may replace a by $a' = a + bt$, for any $t \in R$, we may add any desired element of R to a/b, and in particular assume that the imaginary part y of $a/b = x + iy$ lies (weakly) between $\pm\sqrt{19}/4$. By symmetry it suffices to consider the case $0 \leq y \leq \sqrt{19}/4$.

Now if $0 \leq y < \sqrt{3}/2$, then $p = 1$ will suffice, as then a/b is at distance less than 1 from an ordinary integer. Otherwise, $\sqrt{3}/2 \leq y \leq \sqrt{19}/4$, and we try $p = 2$. Writing y' for the imaginary part of $2a/b - \theta$ we calculate $y' = 2y - \sqrt{19}/2$ and then $\sqrt{3} - \sqrt{19}/2 \leq y' \leq 0$. In order to show that the distance from $2a/b$ to the nearest element of R is strictly less than 1, it suffices to show that $y' > -\sqrt{3}/2$. But $\sqrt{19} < \sqrt{27} = 3\sqrt{3}$, so $-\sqrt{3}/2 < \sqrt{3} - \sqrt{19}/2 < 0$, as required. The result now follows unless $2a/b \in R$, which can only happen when $y = \sqrt{19}/4$.

In this special case, adding ordinary integers to a/b as necessary, we may assume that $a/b = (\pm 1 + \sqrt{19})/4$, and by symmetry these two cases are essentially the same. We now choose $p = (\mp 1 + \sqrt{19})/2$, so that $ap/b = 5/2$ and if $q = 2$ then $|ap/b - q| = 1/4$. □

Acknowledgements

I thank Jérémy Blanc for his interest in this proof, and especially for pointing out that in an earlier version, among other deficiencies, I had failed to consider the final case $2a/b \in R$ in the proof of Lemma 1.

References

[1] T. Motzkin, The Euclidean algorithm, *Bull. Amer. Math. Soc.* **55** (1949), 1142–1146.

[2] Oscar A. Cámpoli, A principal ideal domain that is not a Euclidean domain, *Amer. Math. Monthly* **95** (1988), 868–871.

School of Mathematical Sciences, Queen Mary University of London, Mile End Road, London E1 4NS, U.K.

E-mail address: R.A.Wilson@qmul.ac.uk