An example of a PID which is not a Euclidean domain

R. A. Wilson

11th March 2011; corrected 30th October 2015

Some people have asked for an example of a PID which is not a Euclidean domain. It turns out that $R = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-19})]$ is such an example. I sketch a proof of this here. This is a simplified version of the proof given by Cámpoli [1].

1 R is not a Euclidean domain

First we show that it is not a Euclidean domain. It is obvious that the usual absolute value is not a Euclidean function, but could there be some more exotic Euclidean function?

Let us write $\theta = \frac{1}{2}(1 + \sqrt{-19})$, so that $\theta\overline{\theta} = 5$, and $\theta^2 = \theta - 5$. By explicit calculations rather like the ones we did in lectures for rings like $\mathbb{Z}[\sqrt{-5}]$, we can show that

- The units in R are just 1 and -1.
- The elements 2 and 3 are irreducible in R.

Now suppose there is a Euclidean function d on R. We aim for a contradiction. We choose $m \in R$ such that $d(m)$ is as small as possible, subject to m not being 0 or a unit. First we divide 2 by m, and get a quotient and remainder:

$$2 = mq + r \text{ with } d(r) < d(m) \text{ or } r = 0.$$

This means $r = 0, 1$, or -1. If $r = 0$, then $m|2$, which means $m = \pm 2$, since 2 is irreducible, and m is not a unit. Similarly, if $r = -1$, then $m = \pm 3$. The case $r = 1$ cannot happen, for if it did, then $m|1$ so m is a unit.

Next we divide θ by m in the same way, getting

$$\theta = mq' + r' \text{ with } d(r') < d(m) \text{ or } r' = 0.$$

Again we have $r' = 0, 1$, or -1. So one of θ, $\theta + 1$, or $\theta - 1$ is divisible by m. But $m = \pm 2$ or ± 3, and it is easy to see that none of these quotients is in R. This contradiction tells us that R is not a Euclidean domain for *any* Euclidean function.

2 R is a principal ideal domain

The second part of the proof is to show that R is a PID. We imitate the proof that a Euclidean domain is a PID, but we have to generalise it a little bit. We return to using the usual absolute value as a measure of the size of an element. So pick any non-zero ideal I in R, and let $b \in I$ be chosen so that $b \neq 0$ and $|b|$ is as small as possible. We aim to show that $I = bR$, so suppose not. Then there is an element $a \in I \setminus bR$.

The proof from the lectures proceeds by finding an element $q \in R$ such that $0 < |a - bq| < |b|$, but $a - bq \in I$ so this leads to a contradiction. But more generally we have $ap - bq \in I$ for all $p, q \in R$, so if we can find p, q with $0 < |ap - bq| < |b|$ we will be done.

The proof I found in the literature [1] now divides the proof into seven cases, further subdivided into nine subcases, according to the value of a/b in the complex numbers. However, it seems to me that one only needs to consider two generic cases and one special case. Since we may replace a by any element $a' = a - bq$, we may subtract any desired element of R from a/b. In particular, we can assume that the imaginary part y of $a/b = x + iy$ lies between $\pm\sqrt{19}/4$.

Now if the imaginary part of a/b lies strictly between $\pm\sqrt{3}/2$ then a/b lies at distance less than 1 from some ordinary integer, and we are done. So we may assume the imaginary part of a/b lies between $\sqrt{3}/2$ and $\sqrt{19}/4$ (or the negative of this, where the argument is the same). Hence the imaginary part of $2a/b - (1 + \sqrt{-19})/2$ lies between $\sqrt{3} - \sqrt{19}/2$ and 0. But $\sqrt{19} < \sqrt{27} = 3\sqrt{3}$, so $\sqrt{3}/2 > \sqrt{19}/2 - \sqrt{3} > 0$, so the imaginary part of $2a/b - (1 + \sqrt{-19})/2$ is sufficiently small that the complex number lies at a distance less than 1 from some ordinary integer.

Thus in both cases we have found elements $p, q \in R$ (in fact with $p = 1$ or $p = 2$) such that $|ap - bq| < |b|$. The proof is therefore complete except in the case $ap - bq = 0$, which can only happen when $p = 2$ and $a/b = (1 \pm \sqrt{-19})/4$ modulo the ring. In these cases, choose $p = (1 \mp \sqrt{-19})/2$ instead of $p = 2$, and then $q = 2$, so that $|ap - bq| = 1/2$. This contradicts the assumption that $I \neq bR$. Hence $I = bR$, and because this is true for every non-zero ideal in R, we conclude that R is a PID.

References

[1] Oscar A. Cámpoli, A principal ideal domain that is not a Euclidean domain, Amer. Math. Monthly, vol. 95 no. 9 (Nov. 1988), 868–871.