Math 250A, G. Bergman, 2002

A principal ideal domain that is not Euclidean

developed as a series of exercises

Let α denote the complex number $(1+\sqrt{-19})/2$, and R the ring $\mathbf{Z}[\alpha]$. We shall show that R is a principal ideal domain, but not a Euclidean ring. This is Exercise III.3.8 of Hungerford's *Algebra* (2nd edition), but no hints are given there; the proof outlined here was sketched for me by H. W. Lenstra, Jr..

(1) Verify that $\alpha^2 - \alpha + 5 = 0$, that $R = \{m + n\alpha \mid m, n \in \mathbf{Z}\} = \{m + n\bar{\alpha} \mid m, n \in \mathbf{Z}\}$, where the bar denotes complex conjugation, and that the map $x \mapsto |x|^2 = x\bar{x}$ is nonnegative integer valued and respects multiplication.

(2) Deduce that $|x|^2 = 1$ for all units of R, and using a lower bound on the absolute value of the imaginary part of any non-real member of R, conclude that the only units of R are ± 1.

(3) Assuming R has a Euclidean function φ, let x be a nonzero nonunit of R minimizing $\varphi(x)$. Show that R/xR consists of the images in this ring of 0 and the units of R, hence has cardinality at most 3. What nonzero rings are there of such cardinalities? Show that $\alpha^2 - \alpha + 5 = 0$ has no solution in any of these rings, and deduce a contradiction, showing that R is not Euclidean.

We shall now show that R *is* a principal ideal domain. To do this, let I be any nonzero ideal of R, and x a nonzero element of I of least absolute value, i.e., minimizing the integer $x\bar{x}$. We shall prove $I = xR$. (Thus, we are using the function $x \mapsto x\bar{x}$ as a substitute for a Euclidean function, even though it does not have all the properties of one.)

For convenience, let us ''normalize'' our problem by taking $J = x^{-1}I$. Thus, J is an R-submodule of $\mathbf{C}$, containing R and having no nonzero element of absolute value < 1. We shall show from these properties that $J - R = \emptyset$, i.e., that $J = R$.

(4) Show that any element of J that has distance less than 1 from some element of R must belong to R. Deduce that in any element of $J - R$, the imaginary part must differ from any integral multiple of $\sqrt{19}/2$ by at least $\sqrt{3}/2$. (Suggestion: draw a picture showing the set of complex numbers which the preceding observation excludes. However, unless you are told the contrary, this picture does not replace a proof; it is merely to help you find a proof.)

(5) Deduce that if $J - R$ is nonempty, it must contain an element y with imaginary part in the range $[\sqrt{3}/2,\ \sqrt{19}/2 - \sqrt{3}/2]$, and real part in the range $(-1/2, 1/2]$.

(6) Show that for such a y, the element $2y$ will have imaginary part too close to $\sqrt{19}/2$ to lie in $J - R$. Deduce that $y = \alpha/2$ or $-\bar{\alpha}/2$, and hence that $\alpha\bar{\alpha}/2 \in J$.

(7) Compute $\alpha\bar{\alpha}/2$, and obtain a contradiction. Conclude that R is a principal ideal domain.

(8) What goes wrong with these arguments if we replace 19 throughout by 17? By 23?