Calculus II. Read specified selections from either *The Mathematical Experience* by Davis and Hersh or from *How to Solve It* by Pólya.

Calculus III. Read specified selections from either *Infinity* by Lieber or from *Bridges to Infinity* by Guillen.

Introduction to Linear Algebra. Read three articles from *Scientific American* as follows. Either "Linear Programming," August 1954, or "The Allocation of Resources by Linear Programming," June 1981. One of these articles: "Input-Output Economics", October 1951; "The Structure of U.S. Economy," April 1965; or "The World Economy by the Year 2000," September 1980. One article from the "Mathematics and Modern World" issue of September 1964. ("Math in Social Sciences" is most relevant to this course.)

Introduction to Algebraic Structures. Read either *Flatland* by Abbott, or specified selections from Kline's *Mathematics, The Loss of Certainty* and from Kasner and Newman's *Mathematics and the Imagination*.

A Principal Ideal Domain That Is Not a Euclidean Domain

OSCAR A. CÁMPOLI

Facultad de Matemática, Astronomía y Física, Valparaíso y R. Martínez Ciudad Universitaria, 5000 Córdoba, Argentina

Introduction. In most advanced undergraduate and graduate algebra texts a very simple argument is used to show that a Euclidean domain is a principal ideal domain (PID). And then it is mentioned that the converse is not true, sometimes together with the claim that the subring $A = \mathbb{Z}[\theta] = \{a + b\theta \,|\, a, b \in \mathbb{Z}, \ \theta = (1 + \sqrt{-19})/2\}$ of the complex numbers is a PID but is not a Euclidean domain. I have not been able to find a proof, accessible to beginning graduate students, in any standard reference (e.g., [1, 2, 3, 4]).

In what follows it is shown in an elementary fashion that A has both properties.

The proof that A is not a Euclidean domain is in [5] but we use here a shorter argument suggested by the referee.

One way to see that A is a PID can be found in algebraic number theory books where the class number of the field $\mathbb{Q}(\sqrt{-19})$ is computed. The proof given here uses that A is "almost" a Euclidean domain in the sense that it has a "generalized" Euclidean algorithm. A criterion (sometimes attributed to Dedekind and Hasse) is then proven and used to show that A is a PID.

A is not Euclidean. In general, it is not clearly stated what Euclidean domains are. A definition is as follows:

A *Euclidean domain* consists of an integral domain A together with a map $|\ |: A \to \mathbb{Z}$ (the *Euclidean norm*) that satisfies the following conditions:

(i) $|\ |(a) = |a| \geqslant 0$ for all $a \in A$; $|a| = 0$ if and only if $a = 0$.

(ii) $|ab| = |a| \cdot |b|$ for all $a, b \in A$.

(iii) (Euclidean algorithm) Given $a, b \in A$, $b \neq 0$, there exist $q, r \in A$ so that $a = qb + r$ with $|r| < |b|$.

It is interesting to note that condition (ii) of the definition can be weakened to
  (ii′) $|a| \leqslant |b|$ whenever a divides b (for nonzero b),
which follows easily from (ii). In fact (ii′) will be used instead of (ii).

To show that A is not Euclidean it is sufficient to prove that A does not admit a function $||$ satisfying the three stated properties. Thus assume that $||$ is a Euclidean norm in A. This leads to a contradiction.

Indeed, let U be the set of nonzero elements in A with minimal norm. Since every unit of A divides every nonzero element, (ii′) implies that every unit is in U and (iii) implies that every element of U divides every nonzero element of A; so U consists precisely of the units of A.

We next show that $U = \{1, -1\}$. In order to prove this and other assertions a few specific calculations in the ring A are needed.

The following identities can be proved directly from the definition of $\theta = (1 + \sqrt{-19})/2$. For $a \in A$, $\bar{a}$ denotes the complex conjugate of the complex number a.

  (I) $\bar{\theta} = 1 - \theta$
  (II) $\theta\bar{\theta} = 5$
  (III) $\theta^2 = \theta - 5$
  (IV) For any $x = a + b\theta \in A$, $\theta x = -5b + (a + b)\theta$.

From (I) it follows that A is closed under complex conjugation. Identity (II) implies that the integer 5 is not a prime in A. Later it will be clear that θ is not a unit in A and it will then follow that 5 is reducible in A. From (III) it follows that $\theta^2 \in A$ and hence A is closed under complex multiplication (a fact not obvious from the definition of A).

If $N(z) = z\bar{z}$ is the usual complex norm, then the preceding identities yield:
  (V) $N(a + b\theta) = (a + b\theta)(\overline{a + b\theta}) = a^2 + ab + 5b^2$.
Moreover, the function $N: A \to \mathbb{Z}$ satisfies
  (a) $N(xy) = N(x)N(y)$ for all $x, y \in A$, and
  (b) $N(x) \geqslant 0$ for all $x \in A$ and $N(x) = 0$ if and only if $x = 0$.

This immediately implies that if an element $a + b\theta \in A$ is a unit then $a^2 + ab + 5b^2 = N(a + b\theta) = 1$ and hence, if $ab \geqslant 0$, then $b = 0$ and $a = \pm 1$. Also, since $a + b\bar{\theta} = a + b - b\theta$ and $1 = N(a + b\theta) = N(a + b\bar{\theta}) = (a + b)^2 - ab + 4b^2$, it follows that when $ab \leqslant 0$ then again $b = 0$ and $a = \pm 1$. This concludes the proof of the fact that $U = \{1, -1\}$.

Now assume that m is of minimal norm among the elements of A different from $0, 1, -1$. Condition (iii) implies that $2 = qm + r$, with $|r| < |m|$; therefore r is one of $0, 1$, or -1. Hence either m divides 2 or m divides 3. We claim that m must then be one of $\pm 2, \pm 3$.

This claim is a consequence of the fact that 2 and 3 are primes in A, which is shown as follows. Suppose $2 = (a + b\theta)(c + d\theta)$. Then $4 = N(2) = N(a + b\theta) N(c + d\theta)$ and assuming that $a + b\theta$, $c + d\theta$ are not units in A, it follows that

$$2 = N(a + b\theta) = a^2 + ab + 5b^2 = N(a + b\bar{\theta}) = (a + b)^2 - ab + 4b^2.$$

Therefore, considering the cases $ab \geqslant 0$ and $ab < 0$, we conclude that b and d each equal zero.

Thus $2 = (a + b\theta)(c + d\theta) = ac$ is an integral factorization. Since 2 is a prime in $\mathbb{Z}$, 2 is a prime in A. A similar argument shows that 3 is also a prime in A.

Now, again using (iii), θ is congruent to $0, 1$, or -1 modulo one of ± 2 or ± 3. Hence θ or $\theta - 1$ or $\theta + 1$ is divisible by 2 or 3. But this is impossible since $N(\theta) = 5 = N(\theta - 1)$ and $N(\theta + 1) = 7$, while $N(2) = 4$ and $N(3) = 9$.

A is a **PID.** As stated in the introduction, to show that A is a principal ideal domain (PID) it is enough to show that A is "almost" a Euclidean domain. More precisely, it may be seen that given elements $\alpha, \beta \in A$, $\beta \neq 0$, if β does not divide α and $N(\alpha) \geqslant N(\beta)$ then there exist $\gamma, \delta \in A$ such that

$$0 < N(\alpha\gamma - \beta\delta) < N(\beta). \tag{1}$$

This property implies that A is a PID by an argument similar to the one usually applied to show that $\mathbb{Z}$ is a PID. Let $I \neq 0$ be an ideal in A. Let $\beta \in I$ be an element such that $N(\beta)$ is minimal among the nonzero elements in I. Then $\beta A = I$. Indeed, since clearly $\beta A \subseteq I$, consider the possibility of having an element $\alpha \in I$ such that β does not divide α. Then $\alpha \neq 0$ and hence $N(\alpha) \geqslant N(\beta)$. Now using (i) it is possible to obtain another nonzero element $\alpha\gamma - \beta\delta$ in I which contradicts the minimality of $N(\beta)$.

To show (i) take $\alpha, \beta \in A$, $\beta \neq 0$. If β does not divide α and $N(\alpha) \geqslant N(\beta)$ write

$$\frac{\alpha}{\beta} = a + b\theta,$$

where a and b are rational numbers and at least one of them is not an integer. This is possible since the inverse of β as a complex number is in $\mathbb{Q}[\theta]$, which is a subfield of $\mathbb{C}$.

A case by case consideration leads to elements γ and $\delta \in A$ such that

$$0 < N\left(\frac{\alpha}{\beta}\gamma - \delta\right) < 1, \quad \text{whence} \quad N(\alpha\gamma - \delta\beta) < N(\beta).$$

There are seven cases.

Case 1: $b \in \mathbb{Z}$. Then $a \notin \mathbb{Z}$ and we may take $\gamma = 1$ and $\delta = \{a\} + b\theta$ (here $\{x\}$ denotes the integer nearest x, with $\{n + 1/2\} = n$). Now,

$$0 < N\left(\frac{\alpha}{\beta}\gamma - \delta\right) \leqslant \frac{1}{4} < 1.$$

Case 2(a): $a \in \mathbb{Z}$ *and* $5b \notin \mathbb{Z}$. Then $\dfrac{\alpha}{\beta}\bar{\theta} = a + 5b - a\theta$ and we may take $\gamma = \bar{\theta}$, $\delta = \{a + 5b\} - a\theta$.

Case 2(b): $a \in \mathbb{Z}$ *and* $5b$ $\mathbb{Z}$. Take $\gamma = 1$, $\delta = a + \{b\}\theta$.

Case 3(a): $a, b \notin \mathbb{Z}$ *and* $2a, 2b \in \mathbb{Z}$. Then, although we proved IV for a, $b \in \mathbb{Z}$, it is clearly valid also for a, b rational and hence $\theta\alpha/\beta = -5b + (a + b)\theta$ and $a + b \in \mathbb{Z}$. Therefore, we may take $\gamma = \theta$, $\delta = \{-5b\} + \{a + b\}\theta$.

Case 3(b): $a, b \notin \mathbb{Z}$ *and* $2a, 2b \notin \mathbb{Z}$. Then either $|b - \{b\}| \leqslant 1/3$ or $|2b - \{2b\}| \leqslant 1/3$. In the first situation take $\gamma = 1$ and $\delta = \{a\} + \{b\}\theta$ and estimate

$$0 < N\left(\frac{\alpha}{\beta}\gamma - \delta\right) \leqslant \frac{35}{36} < 1.$$

In the second situation take $\gamma = 2$ and $\delta = \{2a\} + \{2b\}\theta$ with the same estimate.

Case 3(c): $a, b \notin \mathbb{Z}, 2a \in \mathbb{Z}$ and $2b \notin \mathbb{Z}$. When $5b \in \mathbb{Z}$ take $\gamma = 5$ and $\delta = \{5a\} + 5b\theta$ and when $5b \notin \mathbb{Z}$ take $\gamma = 2\bar{\theta}$ and $\delta = \{2a + 10b\} - 2a\theta$.

Case 3(d): $a, b \notin \mathbb{Z}, 2b \in \mathbb{Z}$ and $2a \notin \mathbb{Z}$. Take $\gamma = 2$, $\delta = \{2a\} + 2b\theta$.
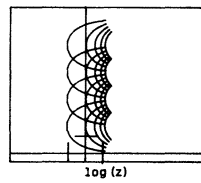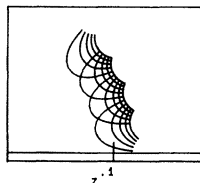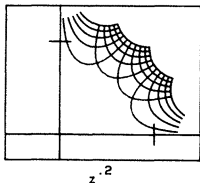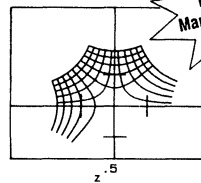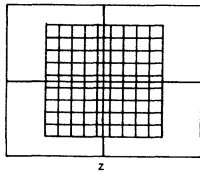
REFERENCES

1. J. Goldhaber and G. Ehrlich, Algebra, Collier Macmillan, London, 1970.
2. T. Hungerford, Algebra, Springer-Verlag, New York, 1974.
3. N. Jacobson, Lectures in Abstract Algebra, Van Nostrand Company Inc., Toronto, 1951.
4. S. Lang, Algebra, Addison-Wesley, Reading, 1965.
5. T. Motzkin, The Euclidean algorithm, *Bull. Amer. Math. Soc.* 55 (1949) 1142–1146.