1. J. E. Littlewood, *Littlewood's Miscellany*, Cambridge University Press, 1986.

Department of Mathematics
Princeton University
Princeton NJ 08544-1000
tokieda@math.princeton.edu

Principal Ideal Domains Are Almost Euclidean

John Greene

In most undergraduate level books on abstract algebra, it is shown that every Euclidean domain (ED) is a principal ideal domain (PID) and every principal ideal domain is a unique factorization domain (UFD). We thus have a set of implications: ED $\Rightarrow$ PID $\Rightarrow$ UFD. Most (but not all!) books mention that neither converse is true. But while it is very easy to show that $Z[x]$ is an example of a UFD that is not a PID, an example of a PID that is not a ED is harder to come by. In [2], Campoli gives an easy proof that $Z[\zeta]$ has the desired properties, where $\zeta = (-1 + \sqrt{-19})/2$, by showing that, in his words, $Z[\zeta]$ is "almost Euclidean." In this note, we show that Campoli's "almost Euclidean" condition is, in fact, equivalent to the PID condition.

Definition. An integral domain D is said to be **almost Euclidean** if there is a function d: $D \to Z^+ \cup \{0\}$ (called an almost Euclidean function) such that

1) $d(0) = 0$, $d(a) > 0$ if $a \neq 0$,
2) If $b \neq 0$, then $d(ab) \geq d(a)$ for all $a \in D$,
3) for any $a, b \in D$, if $b \neq 0$ then either
   i) $a = bq$ for some $q \in D$ or
   ii) $0 < d(ax + by) < d(b)$ for some $x, y \in D$.

Our functions d in this paper will satisfy the stronger condition (2′) that for all a, b in D, $d(ab) = d(a)d(b)$, from which (2) follows trivially.

Our main result is the following:

Theorem 1. *An integral domain D is a principal ideal domain if and only if it is almost Euclidean.*

Proof: Campoli [2] proved that if a ring is almost Euclidean, it is a PID. For completeness, we repeat the proof here. Let D be almost Euclidean, and let I be a nonzero ideal in D. Among the elements $x \in I$, let b be an element with a minimal positive value for $d(x)$. Given $a \in I$, for any $x, y \in D$, $ax + by$ is in I. By definition of b, it cannot be that $0 < d(ax + by) < d(b)$, so the second condition, $a = bq$ must hold for some $q \in D$. Thus, $I = (b)$.

Now suppose that D is a PID. Then D is a UFD, so we may define the function d as follows: Let $d(0) = 0$, and for any $a \neq 0$, if $a = \varepsilon p_1 p_2 \cdots p_n$, where ε is a unit and $p_1, \ldots, p_n$ are irreducibles, let $d(a) = 2^n$. Since $d(ab) = d(a)d(b)$, it is clear that d satisfies (1) and (2) of the definition. So let $a, b \in D$, with $b \neq 0$. Let $I = \{ax + by | x, y \in D\}$. Since I is an ideal in D, $I = \langle r \rangle$ for some $r \in D$ with $r \neq 0$. If $a = bq$ for some $q \in D$, then $I = \langle b \rangle$. Otherwise, $I \neq \langle b \rangle$. Since $b \in I$, $b = xr$ for some $x \in D$, so $d(b) \geq d(r)$. Since $I \neq \langle b \rangle$, x is not a unit. Thus, $d(x) > 1$, so $d(r) < d(b)$. If $r = x_0 a + y_0 b$, then we have $0 < d(r) < d(b)$, and condition (3) is satisfied by d. ∎

Examples of Euclidean domains in abstract algebra texts are almost always of the form $D = F[x]$, where F is a field or the ring of integers in $Q[\sqrt{d}\,]$ for various small integer values of d. In the latter case, these books introduce the norm of an element of this ring and use its absolute value as a Euclidean function. In general, if F is an algebraic number field (a finite extension of Q), then F can be viewed as a finite dimensional vector space over Q. If $a \in F$, then the map $T_a(x) = ax$ is obviously a Q-linear transformation from F to F. The norm of a, $N(a)$, is defined to be the determinant of this transformation. The norm has the following properties:

1) $N(ab) = N(a)N(b)$ for all $a, b \in F$,
2) $N(a) = 0$ if and only if $a = 0$,
3) if a is an algebraic integer, then $N(a) \in Z$,
4) an algebraic integer a is a unit if and only if $N(a) = \pm 1$,

Properties (1) and (2) are elementary properties of determinants, property (3) is mentioned in [**5**, p. 175], and property (4) is an easy consequence of (1), (2), and (3).

Theorem 2. *If D is the set of integers in an algebraic number field, and if D is a principal ideal domain, then the absolute value of the norm satisfies the conditions of an almost Euclidean function.*

Proof: The properties of the function d in Theorem 1 that were used in the proof were:

1) $d(ab) = d(a)d(b)$
2) if $a \in D$, then $d(a) = 1$ if and only if a is a unit.

Since the absolute value of the norm also has these properties, the proof follows as in Theorem 1. Thus, given $a, b \in D$, with $b \neq 0$, let $I = \{ax + by | x, y \in D\} = \langle r \rangle$. If $a = bq$ for some $q \in D$, then $I = \langle b \rangle$. Otherwise, $0 < |N(r)| < |N(b)|$, since $b = xr$ for some nonunit $x \in D$. ∎

If D is the ring of integers in some finite extension F of Q, we may now check if D is a principal ideal domain by checking whether or not D is almost Euclidean with respect to the absolute value of the norm. Thus, number fields are quite special. Another example of this is the following: In a number field, D is a UFD if and only if D is a PID [**6**, page 146]. Campoli [**2**] used the fact that $Z[\zeta\,]$ with $\zeta = (-1 + \sqrt{-19}\,)/2$ is almost Euclidean to show that this ring is a PID. His techniques can be easily extended tc show that this remains true if -19 is replaced by -43 or -163. In fact, with a little work it is possible to prove the famous result

[**1**, p. 137]: The ring of integers in $Q(\sqrt{1-4d})$ where $d > 0$ is a PID if and only if the polynomial $x^2 + x + d$ is prime for all integers x with $0 \le x \le d - 2$.

One final comment: If D is an almost Euclidean subring of a number field, Theorem 2 tells us that we may use the absolute value of the norm as a near Euclidean function. Suppose that D is actually Euclidean. Will the absolute value of the norm serve as a Euclidean function? It is interesting to note that Hardy and Wright [**4**, p. 212] define a Euclidean domain not in the usual way but explicitly using the norm as the Euclidean function. However, the answer to the question is that the norm may not work. In fact, it was shown in [**3**] that $Z[\zeta]$, with $\zeta = (1 + \sqrt{69})/2$ is an example of a ring which is Euclidean, but not with respect to the absolute value of the norm.

ACKNOWLEDGMENTS. I would like to thank Joe Gallian and the reviewer for many helpful comments, and thank the members of the usenet newsgroup sci.math, especially Henry Cohn, for the reference to a ring that is Euclidean but not norm–Euclidean.

REFERENCES

1. Paulo Ribenboim, The Book of Prime Number Records, Springer-Verlag, New York, 1988.
2. Oscar Campoli, A Principal Ideal Domain That Is Not a Euclidean Domain, *American Mathematical Monthly*, **95** (1988) 868–871.
3. David Clark, A quadratic field which is Euclidean but not norm-Euclidean, *Manuscripta Math.* **83** (1994), no. 3-4, 327–330.
4. G. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, 5th Edition, Oxford University Press, Oxford.
5. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1992.
6. Edwin Weiss, *Algebraic Number Theory*, McGraw-Hill, New York, 1963.

A Colorful Determinantal Identity, a Conjecture of Rota, and Latin Squares

Shmuel Onn

1. Rota's Colorful Conjecture and the Latin Square Conjecture. The following conjecture in combinatorial linear algebra is due to Gian-Carlo Rota.

Rota's Colorful Conjecture. Let ${}^1W, \ldots, {}^nW$ be bases of an n-dimensional vector space. Then their multiset union can be repartitioned into bases ${}^1U, \ldots, {}^nU$ such that $|{}^iU \cap {}^jW| = 1$ for all i, j.

Regarding the vectors in each ${}^iW$ as *colored* in color i, the newly sought bases are *colorful*, namely contain one vector of each color. So Rota's Colorful Conjecture is that any n colored bases of an n-dimensional vector space can be repartitioned into n colorful bases.

A *Latin square* of order n is an n by n matrix $L = (L_i^j)$ in which each row and each column is a permutation of $\{1, \ldots, n\}$. More precisely, there are permutations $\sigma_1, \ldots, \sigma_n$ and $\pi_1, \ldots, \pi_n$ such that $L_i^j = \sigma_i(j) = \pi_j(i)$ for all i, j. The *sign* of the Latin square is defined as the product of all signs of its row and column