ACTA ARITHMETICA
LXIV.2 (1993)

A simple characterization of principal ideal domains

by

Clifford S. Queen (Bethlehem, Pa.)

1. Introduction. In this note we give necessary and sufficient conditions for an integral domain to be a principal ideal domain. Curiously, these conditions are similar to those that characterize Euclidean domains. In Section 2 we establish notation, discuss related results and prove our theorem. Finally, in Section 3 we give two nontrivial applications to real quadratic number fields.

2. Results. Let R be an integral domain and K its field of fractions. We say that R is a *principal ideal domain* (abbreviated P.I.D.) if every ideal of R is principal. That is to say, given an ideal ϑ of R there exists β in R such that $\vartheta = (\beta) = \beta R$. A necessary condition for R to be a P.I.D. is that it be factorial or, in other words, that every nonzero element of R can be written uniquely as a product of irreducible elements of R. But being factorial is not sufficient since the polynomial ring in one variable over the integers is factorial but not a P.I.D. (see [2]). A sufficient condition for R to be a P.I.D. is that R be Euclidean (see [7]). We mean by this that there is a map $N : R \to \mathbb{Z}^*$, where $\mathbb{Z}^*$ denotes the nonnegative integers, with the following properties:

(1) $N(\alpha) = 0$ if and only if $\alpha = 0$.

(2) Given α and β in R with $\beta \neq 0$ there exist θ and ϱ in R such that $\alpha = \beta\theta + \varrho$, with $0 < N(\varrho) < N(\beta)$.

Familiar examples of Euclidean domains are the integers, the Gaussian integers and the polynomial ring in one variable over a field. In all of these examples one can choose a map N with the following additional properties: $N(\alpha) = 1$ if and only if α is a unit of R and $N(\alpha\beta) \geq N(\beta)$ for all nonzero α and β in R. It is known (see [7]) that there is no loss of generality in insisting on these additional properties. The ring $\mathbb{Z}[w] = \{x + yw \mid x, y \text{ in } \mathbb{Z}\}$, where

$\mathbb{Z}$ denotes the ring of integers and $w = (1+\sqrt{-19})/2$ is an example of a P.I.D. which is not Euclidean (see [5]).

In the Theorem below we give necessary and sufficient conditions for R to be a P.I.D. These conditions generalize properties discussed by Rabinowitsch and Kutsuna (see [3] and [6]). Recall that $\mathbb{Z}^*$ denotes the nonnegative integers and $\mathbb{Q}^*$ the nonnegative rational numbers.

THEOREM. *Let R be an integral domain and K its field of fractions. Then R is a P.I.D. if and only if there is a map $N : K \to \mathbb{Q}^*$ with the following properties*:

(0) *For all ξ in K, $N(\xi) = 0$ if and only if $\xi = 0$*;
(1) *$N(R)$ is a subset of $\mathbb{Z}^*$*;
(2) *For elements α in R, $N(\alpha) = 1$ if and only if α is a unit*;
(3) *For all ξ and ζ in K, $N(\zeta\xi) = N(\zeta)N(\xi)$*;
(4) *For any ξ in K such that ξ is not in R there exist α and β in R with $0 < N(\xi\alpha - \beta) < 1$.*

Proof. Suppose R is a P.I.D. Our task will be to construct a map N satisfying properties (0) through (4). Let P be a set consisting of one irreducible element for each associate class of irreducible elements of R. If α is a nonzero element of R, let $v(\alpha)$ denote the number of irreducible factors of α taken from P and counting multiplicity. For example, if $\{\pi_1, \pi_2, \ldots, \pi_k\} \subset P$, then $v(\pi_1^{n_1}\pi_2^{n_2}\ldots\pi_k^{n_k}) = n_1 + n_2 + \ldots + n_k$. Since R is factorial, it follows that the map $v : R - \{0\} \to \mathbb{Z}^*$ is well defined and enjoys the following two properties:

(i) $v(\alpha) = 0$ if and only if α is a unit of R;
(ii) $v(\alpha\beta) = v(\alpha) + v(\beta)$ for all α and β in $R - \{0\}$.

Consider the map $N : K \to \mathbb{Q}^*$ defined as follows: If ξ is a nonzero element of K then there exist α and β in R such that $\alpha\beta \neq 0$ and $\xi = \alpha/\beta$. Now define $N(\xi) = 2^{v(\alpha)-v(\beta)}$ and set $N(0) = 0$. Our map satisfies (0) and (1) by definition and properties (2) and (3) are immediate from (i) and (ii).

We need to show that N satisfies property (4). Let ξ be an element of K not in R. Then there exist α and β in R such that $\alpha\beta \neq 0$ and $\xi = \alpha/\beta$. Because R is a P.I.D., there is a nonzero element δ in R such that $(\delta) = \delta R = \alpha R + \beta R$. Since δ divides both α and β, we have $\beta = \delta\nu$, where ν is in R. Further, if ν were a unit of R, then β would divide α, contrary to our assumption. Thus $0 < N(\delta) < N(\delta)N(\nu) = N(\beta)$. Finally, because there exist η and γ in R such that $\delta = \alpha\eta - \beta\gamma$, we have $0 < N(\xi\eta - \gamma) = N(\delta/\beta) < 1$.

Now suppose that N is a map from K to $\mathbb{Q}^*$ satisfying properties (0) through (4). Let ϑ be a nonzero ideal of R and choose β in ϑ such that $N(\beta)$ is minimal over nonzero elements of ϑ. If $N(\beta) = 1$ then β is a unit and $\vartheta = R$, a principal ideal. Next suppose that $N(\beta) > 1$. We will show that $\vartheta = \beta R$ by showing that β divides every element α in ϑ. To that end, let α be in ϑ and assume that β does not divide α. Then it follows that $\xi = \alpha/\beta$ is in K but not in R. So by property (4) there exist η and γ in R with $0 < N(\xi\eta - \gamma) < 1$, i.e. $0 < N(\alpha\eta - \beta) < N(\beta)$. Now since $\alpha\eta - \beta\gamma$ is a nonzero element of ϑ, we have a contradiction to the minimality of $N(\beta)$. ∎

COROLLARY. *If R is a P.I.D. and $N : K \to \mathbb{Q}^*$ satisfies properties* (1) *through* (3) *above*, *then property* (4) *is also satisfied.*

Proof. This is just the first part of the proof of the Theorem. ∎

3. Applications. To show that our necessary and sufficient condition is not impossible to use, we present easy proofs of two well known results.

PROPOSITION. *Let p be a rational integer prime such that $p \equiv 5 \pmod 8$. Consider the ring $R = \mathbb{Z}[\sqrt{2p}]$. Then R is not a P.I.D.*

Proof. It is well known that R is the ring of integers in $K = \mathbb{Q}(\sqrt{2p})$ (see [1]). The absolute value of the norm map from K to $\mathbb{Q}$ is given by $N(s + t\sqrt{2p}) = |s^2 - 2pt^2|$, where s and t are in $\mathbb{Q}$. Now it is easy to show that N satisfies properties (0) through (3). So if R were a P.I.D. then, by the above corollary and the fact that $\sqrt{2p}/2$ is not in R, there would exist $x + y\sqrt{2p}$ and $z + w\sqrt{2p}$ in R such that $0 < N(\sqrt{2p}(x + y\sqrt{2p}) - 2(z + w\sqrt{2p})) = |(2py - 2z)^2 - 2p(x - 2w)^2| < 4$. That is $0 < |2(py - z)^2 - p(x - 2w)^2| < 2$ and so $2(py - z)^2 - p(x - 2w)^2 = \pm 1$. Therefore $2z^2 \equiv \pm 1 \pmod p$ and by the assumption on p this is impossible. ∎

PROPOSITION. *Suppose p is a rational integer prime with $p \equiv 5 \pmod 8$ and $p > 5$. Consider the ring $\mathbb{Z}[\omega]$, where $\omega = (1 + \sqrt{5p})/2$. Then R is not a P.I.D.*

Proof. Our map is the absolute value of the norm from $K = \mathbb{Q}(\omega)$ to $\mathbb{Q}$ given by $N(s + t\omega) = |s^2 + st - t^2(5p - 1)/2|$, where s and t are in $\mathbb{Q}$. Since $\omega/2$ is not in R, if R were a P.I.D. there would exist elements $x + y\omega$ and $z + w\omega$ in R such that

$$0 < N(\omega(x + y\omega) - 2(z + w\omega)) < 4\,.$$

That is to say,

$$\begin{aligned}0 < |(-2z + y(5p-1)/4)^2 + (-2z + y(5p-1)/4)(x + y - 2w)&\\ -(x + y - 2w)^2(5p-1)/4| < 4\,.&\end{aligned}$$

Now if $p = 8k + 5$, then $(5p - 1)/4 = 2(5k + 3)$ and thus

$$2(-z+y(5k+3))^2 + (-z+y(5k+3))(x+y-2w) - (x+y-2w)^2(5k+3) = \pm 1\,.$$

Now setting $A = -z + y(5k+3)$, $B = x + y - 2w$ and computing modulo 5 we have

$$2A^2 + AB - 3B^2 \equiv 2(A-B)^2 \equiv \pm 1 \pmod 5,$$

which is clearly impossible. ■

References

[1] H. Cohn, *Advanced Number Theory*, Dover, 1980.
[2] N. Jacobson, *Basic Algebra I*, 2nd ed., Freeman, 1985.
[3] M. Kutsuna, *On a criterion for the class number of a real quadratic field to be one*, Nagoya Math. J. 79 (1980), 123–129.
[4] T. Motzkin, *The Euclidean algorithm*, Bull. Amer. Math. Soc. 55 (1949), 1142–1146.
[5] C. Queen, *Arithmetic euclidean rings*, Acta Arith. 26 (1974), 105–113.
[6] G. Rabinowitsch, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern*, J. Reine Angew. Math. 142 (1913), 153–164.
[7] P. Samuel, *About Euclidean rings*, J. Algebra 19 (1971), 282–301.

DEPARTMENT OF MATHEMATICS
LEHIGH UNIVERSITY
BETHLEHEM, PENNSYLVANIA. 18015
U.S.A.
E-mail: CSQ0@LEHIGH.EDU

Received on 18.12.1991
and in revised form on 20.11.1992 (2207)