JOURNAL OF NUMBER THEORY 5, 132–138 (1973)

# Prüfer Rings*

PAUL CAMION

*Department of Mathematics, University of Toulouse, Toulouse, France*

L. S. LEVY

*Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706*

AND

H. B. MANN

*Department of Mathematics, University of Arizona, Tucson, Arizona 85721*

Communicated February 7, 1971

A short exposition of the most important properties of Prüfer rings is given. The use of the axiom of choice is avoided whenever this is possible.

In the following we prove some of the properties of Prüfer rings.

DEFINITION 1. An ideal $\mathfrak{a}$ in a ring $R$ is called invertible if there exists an ideal $\mathfrak{b} \subset R$ such that $\mathfrak{ab} = (\alpha)$, a nonzero principal ideal.

DEFINITION 2. An integral domain $R$ is called a Prüfer ring (multiplication ring in the older literature) if every finitely generated (f.g.) ideal has an inverse.

If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals then their g.c.d. $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$ where $\mathfrak{a} + \mathfrak{b} = \{a + b; a \in \mathfrak{a}, b \in \mathfrak{b}\}$.

If $a$, $b$ are elements of $R$ then we set

$$(a) + (b) = (a, b).$$

In the following small latin or greek letters $a, b, c \cdots \alpha, \beta, \gamma \cdots$ will denote elements of a ring $R$ while German letters $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ will denote ideals of $R$.

We shall prove several properties of Prüfer rings. In the proofs of (P1)–(P4) $R$ will denote a Prüfer ring. We shall give proofs which avoid using the axiom of choice either directly or indirectly.

* Sponsored by the Mathematics Research Center United States Army, Madison, Wisconsin, under contract No. DA-31-124-ARD-D462.

PROPERTY 1 (P1). *If* $\mathfrak{a}$ *is f.g. and* $\mathfrak{ab} = \mathfrak{ac}$ *then* $\mathfrak{b} = \mathfrak{c}$.

*Proof.* Let $\mathfrak{a}\bar{\mathfrak{a}} = (\alpha)$. Then $\alpha\mathfrak{b} = \alpha\mathfrak{c}$ hence $\mathfrak{b} = \mathfrak{c}$.
The property (P1) is called the finite cancellation law (fcl).

PROPERTY 2. (P2). *If* $\mathfrak{a} \supset \mathfrak{b}$ *and* $\mathfrak{a}$ *is f.g. then* $\mathfrak{a}$ *divides* $\mathfrak{b}$ ($\mathfrak{b} = \mathfrak{ac}$ *for some* $\mathfrak{c}$).

*Proof.* Let $\bar{\mathfrak{a}}\mathfrak{a} = (\alpha)$. Then $\mathfrak{a} \supset \mathfrak{b}$ implies $(\alpha) \supset \bar{\mathfrak{a}}\mathfrak{b}$. Hence

$$\bar{\mathfrak{a}}\mathfrak{b} = (\alpha)\mathfrak{c} = \mathfrak{a}\bar{\mathfrak{a}}\mathfrak{c}$$

and by (P1)

$$\mathfrak{b} = \mathfrak{ac}.$$

PROPERTY 3 (P3). *If* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ *are f.g. then*

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}. \tag{1}$$

*Proof.* In any commutative ring $R$

$$(\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b}) \subseteq \mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}. \tag{2}$$

If $(\mathfrak{a}, \mathfrak{b}) = 1$ then (2) implies $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$.
By (P2) and (P1)

$$\mathfrak{a} = (\mathfrak{a} + \mathfrak{b})\,\mathfrak{a}_1\,, \qquad \mathfrak{b} = (\mathfrak{a} + \mathfrak{b})\,\mathfrak{b}_1\,, \qquad (\mathfrak{a}_1\,, \mathfrak{b}_1) = 1.$$

In any ring

$$(\mathfrak{a} \cap \mathfrak{b})\mathfrak{c} \subset \mathfrak{ac} \cap \mathfrak{bc}.$$

Hence in a Prüfer ring

$$\begin{aligned}\mathfrak{a} \cap \mathfrak{b} &= ((\mathfrak{a} + \mathfrak{b})\,\mathfrak{a}_1 \cap (\mathfrak{a} + \mathfrak{b})\,\mathfrak{b}_1) \supset (\mathfrak{a} + \mathfrak{b})(\mathfrak{a}_1 \cap \mathfrak{b}_1) \\ &= (\mathfrak{a} + \mathfrak{b})\,\mathfrak{a}_1\mathfrak{b}_1\,.\end{aligned}$$

Multiplying this by $\mathfrak{a} + \mathfrak{b}$ we get

$$(\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b}) \supset \mathfrak{ab} \tag{3}$$

and on account of (2)

$$(\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b}) = \mathfrak{ab}. \tag{4}$$

Now if $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ are f.g. we have by (4)

$$[\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c})](\mathfrak{a} + \mathfrak{b} + \mathfrak{c}) = \mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{ab} + \mathfrak{ac}. \tag{5}$$

Hence $\mathfrak{a} + \mathfrak{b} + \mathfrak{c}$ divides $\mathfrak{ab} + \mathfrak{ac}$ and

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \frac{\mathfrak{ab} + \mathfrak{ac}}{\mathfrak{a} + \mathfrak{b} + \mathfrak{c}}. \tag{6}$$

It is easily checked by cross multiplication that

$$\frac{\mathfrak{ab} + \mathfrak{ac}}{\mathfrak{a} + \mathfrak{b} + \mathfrak{c}} = \frac{\mathfrak{ab}}{\mathfrak{a} + \mathfrak{b}} + \frac{\mathfrak{ac}}{\mathfrak{a} + \mathfrak{c}}. \tag{7}$$

(To establish the identity

$$(\mathfrak{ab} + \mathfrak{ac})(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) = (\mathfrak{ab}(\mathfrak{a} + \mathfrak{c}) + \mathfrak{ac}(\mathfrak{a} + \mathfrak{b}))(\mathfrak{a} + \mathfrak{b} + \mathfrak{c}) \tag{8}$$

observe that all terms $\mathfrak{a}^i\mathfrak{b}^j\mathfrak{c}^k$, $1 \leqslant i \leqslant 3, 0 \leqslant j \leqslant 2, 0 \leqslant k \leqslant 2\, i + j + k = 4$ occur on both sides of (8).) Combining (7), (6), and (4) now gives (1) and proves (P3).

Let $F$ be the quotient field of $R$ and $\mathfrak{p}$ a maximal ideal of $R$. Let $R_{\mathfrak{p}}$ consist of all elements of $F$ which may be written with denominator prime to $\mathfrak{p}$. The ring $R_{\mathfrak{p}}$ is called the localization of $R$ at $\mathfrak{p}$.

PROPERTY 4 (P4). *Every localization of $R$ is a valuation ring. (If $a, b \in R_{\mathfrak{p}}$ then either $a$ divides $b$ or $b$ divides $a$.)*

*Proof.* If $\mathfrak{ab} = (\alpha)$ then $\mathfrak{a}$ and $\mathfrak{b}$ are f.g. For

$$\alpha = \sum_{i=1}^{t} \sum_{j=1}^{s} \lambda_{ij}\alpha_i\beta_j .$$

Hence

$$\alpha = (\alpha_1, \ldots, \alpha_t)(\beta_1, \ldots, \beta_s) = (\alpha_1, \ldots, \alpha_t)\mathfrak{b}$$

since $\beta\alpha_j \equiv 0(\alpha)$ for all $\beta \in \mathfrak{b}$. Now multiply by $\mathfrak{a}$ to get

$$\alpha\mathfrak{a} = (\alpha_1, \ldots, \alpha_t)\alpha.$$

Hence

$$\mathfrak{a} = (\alpha_1, \ldots, \alpha_t).$$

Now let

$$a = (a, b)\mathfrak{a},\ b = (a, b)\mathfrak{b}$$

where $\mathfrak{a} + \mathfrak{b} = 1$ and $\mathfrak{a}$ and $\mathfrak{b}$ are f.g. Then either $\mathfrak{a} + \mathfrak{p} = 1$ or $\mathfrak{b} + \mathfrak{p} = (1)$. We arrange the notation so that $\mathfrak{b} + \mathfrak{p} = (1)$. Then $\mathfrak{b} \ni \beta$ where $\beta \notin \mathfrak{p}$. Let $\mathfrak{b}\bar{\mathfrak{b}} = (\beta)$ then

$$a\bar{\mathfrak{b}} = (a, b)\,\mathfrak{a}\bar{\mathfrak{b}}, \qquad b\bar{\mathfrak{b}} = (a, b)\beta;$$

cross multiplication and division by $(a, b)\bar{\mathfrak{b}}$ gives

$$a\beta = b\mathfrak{a}\bar{\mathfrak{b}}.$$

This shows that $\mathfrak{a}\bar{\mathfrak{b}}$ is principal $\mathfrak{a}\bar{\mathfrak{b}} = (\alpha)$ and $\alpha$ can be chosen so that

$$a/b = \alpha/\beta \quad (\beta, \mathfrak{p}) = 1.$$

Hence $a/b \in R_{\mathfrak{p}}$. This proves (P4).

Each of the Properties (P1)–(P4) characterize Prüfer rings. In proving this for (P1)–(P3) we shall avoid the axiom of choice. Hence we shall not assume that every ideal is contained in a maximal ideal. In proving the converse of (P4) the axiom of choice will be assumed.

We first prove the following lemma.

LEMMA 1. *Let $R$ be a commutative ring. If $(a, b)$ has an inverse for any $a, b \in R$ then every f.g. ideal has an inverse.*

*Proof.* Let $\mathfrak{m}$ be generated by $m \geqslant 3$ elements. Then we may write

$$\mathfrak{m} = \mathfrak{a} + \mathfrak{b} + \mathfrak{c}$$

where $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ have at least one and at most $m - 2$ generators. It is easy to check that

$$\begin{aligned}(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c})(\mathfrak{b} + \mathfrak{c}) &= (\mathfrak{a} + \mathfrak{b} + \mathfrak{c})(\mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}) \\ &= \mathfrak{m}(\mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}).\end{aligned}$$

By induction we may assume that $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{a} + \mathfrak{c}$, $\mathfrak{b} + \mathfrak{c}$ have inverses and so

$$\mathfrak{m}(\mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c})(\mathfrak{a} + \mathfrak{b})^{-1}(\mathfrak{a} + \mathfrak{c})^{-1}(\mathfrak{b} + \mathfrak{c})^{-1} = (\gamma)$$

a principal ideal. Q.E.D.

We first prove the converse to (P1). It is easy to see that fcl holds for the ideals of an integral domain $J$ if and only if it holds for the fractional ideals of its quotient field $Q$. Let $\omega \in Q$. We have

$$(1, \omega)(1, \omega^2) \supset (1, \omega)\omega$$

hence by fcl

$$(1, \omega^2) \ni \omega$$

or

$$\begin{aligned}\omega &= c + d\omega^2 \qquad c, d \in J. \\ 1 &= c\omega^{-1} + d\omega.\end{aligned}$$

Therefore,

$$c\omega^{-1}(1, \omega) = (1 - d\omega, c) \subset (1, \omega)$$

and by fcl

$$c\omega^{-1} \in (1).$$

Whence

$$(1, \omega)(c\omega^{-1}, d) = (1).$$

This proves that $(1, \omega)$ has an inverse and that in general $(a, b)$ has an inverse for any $a, b \in R$. Hence by Lemma 1 every f.g. ideal has an inverse.

It is worth noting that fcl implies integral closure. Suppose that fcl holds in $J$ and suppose $\xi$ is integral over $J$ and in the quotient field $Q$ of $J$. Set

$$\mathfrak{n} = (1, \xi, \ldots).$$

Then $\mathfrak{n}$ is f.g. and $\mathfrak{n}^2 = \mathfrak{n}$ and fcl implies $\mathfrak{n} = 1$, hence $\xi \in J$.

The converse to (P2) is obvious. If $\mathfrak{a} \supset \alpha$ and is f.g. then $\mathfrak{ab} = (\alpha)$ for some $\mathfrak{b}$ if (P2) holds in $J$. Hence $J$ is a Prüfer ring.

If (P3) holds in $J$ then $a \in (a) \cap (b, a - b) = ((a) \cap (b), (a) \cap (a - b))$. Hence the system of congruences

$$x \equiv 0(a), \qquad x \equiv 0(b), \qquad x \equiv a(a - b) \tag{9}$$

is solvable for any pair of elements $a, b$ of $J$. Hence we can find

$$x = \lambda a = \mu b = a + \mu_1(a - b). \tag{10}$$

We then have

$$(a, b)(\mu, \mu_1) = a.$$

Hence $(a, b)$ has an inverse and by Lemma 1 every finitely generated ideal has an inverse.

To prove that (P4) implies the Prüfer property we shall show that (P4) implies (P1). Suppose

$$\mathfrak{ab} = \mathfrak{ac}.$$

Then for every maximal ideal $\mathfrak{p}$

$$\mathfrak{a}_\mathfrak{p}\mathfrak{b}_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}\mathfrak{c}_\mathfrak{p}.$$

If $\mathfrak{a}$ is f.g. and $R_\mathfrak{p}$ is a valuation ring then $\mathfrak{a}_\mathfrak{p}$ is principal hence

$$\mathfrak{b}_\mathfrak{p} = \mathfrak{c}_\mathfrak{p}$$

for every $\mathfrak{p}$. If $\beta \in \mathfrak{b}$, we therefore have

$$s^{(\mathfrak{p})}\beta = c^{(\mathfrak{p})}, \qquad s^{(\mathfrak{p})} \in J, \qquad c^{(\mathfrak{p})} \in \mathfrak{c}, \qquad (s^{(\mathfrak{p})}, \mathfrak{p}) = 1. \tag{11}$$

Since the $s^{(\mathfrak{p})}$ are not all contained in any maximal ideal they must (on account of Zorn's lemma) generate $R$ hence

$$\sum \lambda^{(\mathfrak{p})} s^{(\mathfrak{p})} = 1$$

where the summation extends over a finite number of maximal ideals. Multiplying (11) by $\lambda^{(\mathfrak{p})}$ and summing gives

$$\beta \in \mathfrak{c}.$$

Hence $\mathfrak{b} \subseteq \mathfrak{c}$ and similarly $\mathfrak{c} \subseteq \mathfrak{b}$ hence $\mathfrak{b} = \mathfrak{c}$.

We shall now give a short proof of the so-called globalization theorem. To prove this theorem in all generality one can extend the definition of localization to rings with zero divisors and to all modules.

Let $G$ be a module over $R$ and let $\mathfrak{p}$ be a prime ideal of $R$. We introduce fractions $g/y$ with $g \in G$ and $(y, \mathfrak{p}) = 1$. We define an equivalence relation

$$g/y \sim g_1/y_1 . \tag{12}$$

If there is an $S \in R$, $(S, \mathfrak{p}) = 1$ such that

$$S(y_1 g - y g_1) = 0.$$

We also define

$$(g/y) + (g_1/y_1) = (y_1 g + y g_1)/y y_1 , \qquad a(g/y) = (ag/y) \qquad \text{for} \quad a \in R.$$

It is not difficult to check that (12) is indeed an equivalence relation and that the equivalence classes form a module $G_{\mathfrak{p}}$ over $R$.

Now assume that $M$ and $N$ are modules over $R$ and that we have a linear mapping $\sigma(M) \to N$. We extend $\sigma$ to a mapping $\sigma_{\mathfrak{p}}$ of $M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ setting

$$\sigma_{\mathfrak{p}}(m/y) = \sigma m/y. \tag{13}$$

We shall prove the following.

THEOREM 1 (The globalization theorem). *Let $M$ and $N$ be modules over a commutative ring $R$ and $\sigma$ a linear mapping of $M$ into $N$. Then $\sigma$ is surjective, injective, or 0 if and only if $\sigma_{\mathfrak{p}}$ is surjective, injective, or 0 for each maximal ideal $\mathfrak{p}$.*

*Proof.* If $\sigma$ is surjective or 0 then $\sigma_{\mathfrak{p}}$ is obviously surjective or 0 for every $\mathfrak{p}$. If $\sigma$ is injective and $\sigma_{\mathfrak{p}}(m/y) = \sigma(m)/y \sim 0$ then $s\sigma(m) = 0$ hence $\sigma(sm) = 0$. Therefore $sm = 0$ for $(s, \mathfrak{p}) = 1$ and this means $m \sim 0$ in $M_{\mathfrak{p}}$.

We proceed to prove the sufficiency of the conditions of Theorem 1. (The axiom of choice and hence Zorn's lemma will be assumed in the proof.)

*Case* 1. Let $\sigma_{\mathfrak{p}}$ be surjective then

$$\sigma_{\mathfrak{p}}(m/y) \sim n, \qquad (y, \mathfrak{p}) = 1$$

is solvable for every $n \in N$. Hence

$$s^{(\mathfrak{p})}(\sigma(m) - y^{(\mathfrak{p})}n) = 0.$$

Since $\sigma$ is a linear mapping this shows that the equation

$$\sigma(m) = s^{(\mathfrak{p})}n \tag{14}$$

is solvable for $m$ and $s^{(\mathfrak{p})}$ in $R$ and $(s^{(\mathfrak{p})}, \mathfrak{p}) = 1$. The $s^{(\mathfrak{p})}$ are relatively prime in their totality, hence (Zorn's lemma)

$$\sum \lambda_{\mathfrak{p}} s^{(\mathfrak{p})} = 1 \tag{15}$$

where the sum extends over a finite number of $\mathfrak{p}$. Multiplying (14) by $\lambda_{\mathfrak{p}}$ and summing yields a solution to

$$\sigma(m) = n$$

with $m \in R$.

*Case* 2. Suppose $\sigma_{\mathfrak{p}}(m) = 0$ for all $\mathfrak{p}$. Then we can solve $s^{(\mathfrak{p})}\sigma(m) = 0$, with $(s^{(\mathfrak{p})}, \mathfrak{p}) = 1$ and $\sigma(m) = 0$ follows as in Case 1.

*Case* 3. Suppose that $\sigma^{(\mathfrak{p})}$ is injective for every $\mathfrak{p}$ and suppose $\sigma(m) = 0$. Since $\sigma^{(\mathfrak{p})}$ is injective for every $\mathfrak{p}$ we must have

$$m \sim 0$$

in $M_{\mathfrak{p}}$ for every $\mathfrak{p}$. This means

$$s^{(\mathfrak{p})}m = 0, \qquad (s^{(\mathfrak{p})}, \mathfrak{p}) = 1$$

is solvable for $s^{(\mathfrak{p})}$ for every $\mathfrak{p}$ and it follows as before that $m = 0$. Hence $\sigma$ is injective.

This completes the proof of Theorem 1.

Theorem 1 together with (P4) gives almost immediately (P3). The proof of Theorem 1 however assumes Zorn's lemma hence the axiom of choice while the proof of (P3) given here is free of this assumption.