

ON CHARACTERIZATIONS OF PRÜFER RINGS

CHR. U. JENSEN

According to the classical definition a Prüfer ring is an integral domain R in which the set of all finitely generated non-zero ideals forms a multiplicative group, or, equivalently, any finitely generated ideal $\neq (0)$ is invertible (or projective considered as an R -module).

In recent years it has turned out that Prüfer rings appear in a very natural way in some important concepts of homological algebra as for instance the functors Tor_n , $n = 1, 2$, and thereby tensor products of torsion-free modules, cf. Hattori [4], where Prüfer rings are characterized in terms of homological algebra.

It therefore might be of some interest to give some further characterizations in terms of entirely ideal-theoretical notions. In particular in the case of Noetherian domains we thus obtain characterizations of Dedekind domains some of which were first found by I. S. Cohen [1].

The first characterization which we shall give here refers to the lattice formed by all ideals in R (ordered with respect to set inclusion). In fact, we prove the following

THEOREM 1. *An integral domain R is a Prüfer ring if and only if the lattice formed by ideals of R is distributive, i.e.*

$$a \cap (b + c) = a \cap b + a \cap c$$

for any three ideals in R .

REMARK. Rings in which the lattice of ideals is distributive have been discussed by L. Fuchs [3]. The theorem shows that "arithmetical" domains in the sense of Fuchs actually are Prüfer rings.

For the proof of this and some of the next theorems we shall be using the following well-known result a simple proof of which may be found in Jaffard [5].

LEMMA 1. *An integral domain R is a Prüfer ring if and only if the quotient ring $R_{\mathfrak{p}}$ is a valuation ring for any maximal ideal \mathfrak{p} .*

An ideal α in R is uniquely determined by its local components $\alpha_{\mathfrak{p}}$ which is an immediate consequence of $\alpha = \bigcap_{\mathfrak{p}} \alpha_{\mathfrak{p}}$, \mathfrak{p} running through the maximal ideals in R . Since the formation of sums and intersections of ideals is preserved by extensions of ideals from R to $R_{\mathfrak{p}}$, in view of lemma 1 the “only if” part of theorem 1 is clear once it has been proved for local domains. (Here and in the following the use of the word local should not involve any assumptions of the ring being Noetherian.) The “only if” part of theorem 1 is now obvious, because the ideals in a valuation ring are totally ordered by set inclusion.

To prove the second part of theorem 1 we first point out that the distributive law for R 's ideals is inherited by any quotient ring R_S , S being a multiplicative system. In fact, let α' , \mathfrak{b}' and \mathfrak{c}' be arbitrary ideals in R_S and α , \mathfrak{b} and \mathfrak{c} their respective contractions to R . We only have to prove

$$\alpha' \cap (\mathfrak{b}' + \mathfrak{c}') \subseteq \alpha' \cap \mathfrak{b}' + \alpha' \cap \mathfrak{c}'$$

since the converse inclusion is satisfied for any commutative ring.

Any element x in $\alpha' \cap (\mathfrak{b}' + \mathfrak{c}')$ admits representations

$$x = a/s_1, \quad a \in \alpha, \quad s_1 \in S; \quad x = b/s_2 + c/s_3, \quad b \in \mathfrak{b}, \quad c \in \mathfrak{c}, \quad s_2, s_3 \in S.$$

Since $s_1 s_2 s_3 x \in \alpha \cap (\mathfrak{b} + \mathfrak{c})$,

$$s_1 s_2 s_3 x = u + v, \quad u \in \alpha \cap \mathfrak{b}, \quad v \in \alpha \cap \mathfrak{c},$$

which shows the desired inclusion, $s_1 s_2 s_3$ being a unit in R_S . The “if” part of theorem 1 therefore is contained in the following lemma which we with a view to a later application set up in a slightly more general form by admitting zero-divisors.

LEMMA 2. *The ideals of a local ring R with a distributive lattice of ideals are totally ordered by set inclusion.*

PROOF. It is clearly sufficient to show that for any two non-zero elements a and b , at least one of the statements $a \mid b$ or $b \mid a$ will be true.

In fact, since the ideals are assumed to form a distributive lattice we have

$$(a) = (a) \cap [(b) + (a - b)] = (a) \cap (b) + (a) \cap (a - b)$$

so that a may be written in the form

$$a = t + (a - b)c,$$

where t is an element in $(a) \cap (b)$ and $b \cdot c$ an element in (a) . If c is a unit, b is a multiple of bc and thus belongs to (a) . If c is not a unit, $1 - c$ must be a unit since the ring considered is local (the non-units form R 's unique

maximal ideal). Therefore a is a multiple of $a(1-c) = t - bc$, which is an element in (b) . This means that either $a \mid b$ or $b \mid a$.

We shall now give an application of theorem 1, or more precisely of lemma 2, concerning a simple characterization of Dedekind domains. It is a classical theorem that every proper ideal in a Dedekind domain has a basis consisting of two elements. This property is not characteristic of Dedekind domains, as shown by non-maximal orders in quadratic extensions of the rational number field. The stronger property enjoyed by a Dedekind domain R that any proper residue class ring R/\mathfrak{a} , $\mathfrak{a} \neq (0)$ is a principal ideal ring, however turns out to be characteristic. We state this as

THEOREM 2. *An integral domain R is a Dedekind domain if and only if any proper residue class ring R/\mathfrak{a} , $\mathfrak{a} \neq (0)$ is principal ideal ring.*

PROOF. Let R be an integral domain for which any proper residue class ring is a principal ideal ring. R is then necessarily a Noetherian domain, and it suffices to show that R is a Prüfer ring, since this will imply that every non-zero ideal is invertible. By lemma 1 we have to prove that any quotient ring $R_{\mathfrak{p}}$, \mathfrak{p} being a maximal ideal, is a valuation ring.

Let a and b be two arbitrary elements $\neq 0$ in R . Since the property that any proper residue class ring is principal ideal ring clearly is inherited by the quotient rings, in particular, the residue class ring $R_{\mathfrak{p}}/(a \cdot b)$ must be a principal ideal ring.

The lattice of ideals in any principal ideal ring is distributive. This may be seen either directly or by Krull's theorem that any principal ideal ring is a direct sum of principal ideal domains and of "special" principal ideal rings (i.e. local rings with nilpotent maximal ideals).

Consequently the residue class ring $R_{\mathfrak{p}}/(a \cdot b)$ is a local ring whose ideals form a distributive lattice, and are therefore (by lemma 2) totally ordered with respect to set inclusion. For the ideals $(a)/(ab)$ and $(b)/(ab)$ in $R_{\mathfrak{p}}/(ab)$ this means that at least one is contained in the other, implying that we inside $R_{\mathfrak{p}}$ have $(a) \subseteq (b)$ or $(b) \subseteq (a)$. This shows that $R_{\mathfrak{p}}$ is a valuation ring, since any principal ideal in $R_{\mathfrak{p}}$ may be generated by an element in R .

The "only if" part of the theorem being well known, theorem 2 is now proved.

REMARK. By the same method it can be shown that an integral domain R is a Prüfer ring if any proper residue class ring R/\mathfrak{a} , $\mathfrak{a} \neq (0)$ is a Bezout ring (i.e. a ring in which any finitely generated ideal is principal.) This result, however only yields a sufficient condition for R to be a Prüfer

ring. In fact, if K is an algebraic number field for which the number h of ideal classes is greater than 1, the subset of $K[[X]]$, consisting of all formal power series whose constant terms are algebraic integers, will form a Prüfer ring R for which the residue class ring $R/(X)$ is no Bezout ring.

Next we establish two characterizations of Prüfer rings involving the multiplicative structure of ideals, namely

THEOREM 3. *The integral domain R is a Prüfer ring if and only if one of the following equivalent conditions is satisfied:*

- I. $a \cdot (b \cap c) = a \cdot b \cap a \cdot c$ for any three ideals in R .
- II. $(a + b) \cdot (a \cap b) = ab$ for any three ideals in R .

PROOF. Since the formation of sums, products and intersections of ideals is preserved by extension from R to a quotient ring R_p , the properties I and II at once follows for Prüfer rings, because in this case R_p is a valuation ring for any maximal p and the ideals in R_p thus totally ordered by set inclusion.

To complete the proof we show that I implies II, and II implies that R is a Prüfer ring.

Suppose I holds; then

$$(a + b) \cdot (a \cap b) = (a + b)a \cap (a + b)b \cong ab .$$

Comparing this with the converse inclusion $(a + b)(a \cap b) \subseteq ab$ valid for any commutative ring, we obtain II.

If II holds we shall show that any finitely generated ideal $\neq (0)$ is invertible. We shall do this by induction with respect to the number n of generators.

If $n = 1$ the ideals considered are principal and therefore invertible. Let us assume that any ideal generated by $(n - 1)$ elements has been proved to be invertible. Let $c = (c_1, \dots, c_n)$ be an arbitrary ideal generated by n non-zero elements. Putting $a = (c_1, \dots, c_{n-1})$ and $b = (c_n)$ we have

$$c \cdot (a \cap b) = ab$$

which shows that c is invertible since a and b were assumed to be so and products and factors of invertible ideals are invertible.

REMARK. The relations I, II and the distributive law expressed in theorem 1 have a meaning in any lattice-ordered semigroup, but are in general not equivalent, as may be shown by simple examples.

We shall now give two simple applications of theorem 3. The first one

generalizes the well-known theorem that a Dedekind domain with unique factorization is a principal ideal domain, namely

COROLLARY 1. *Any Prüfer ring with unique factorization is a principal ideal domain.*

PROOF. It suffices to show that the greatest common divisor d of any two elements a and b ($\neq 0$) may be expressed as a linear combination of a and b . Dividing by d we may well assume that a and b are relatively prime, so that $(a) \cap (b) = (a \cdot b)$. By property II of theorem 3 we obtain $(a, b) \cdot (ab) = (ab)$ and thus $(a, b) = R = (1)$.

As a second application we shall give the following characterization of Dedekind domains:

COROLLARY 2. *An integrally closed domain R is a Dedekind domain if and only if any ideal in R is an intersection of finitely many fractionary principal ideals.*

PROOF. The “only if” part is well known. To prove the “if” part we notice that the assumption that any ideal \mathfrak{a} may be expressed as an intersection of principal ideals involves that $\mathfrak{a} = \mathfrak{a}_v$ where \mathfrak{a}_v denote the v -ideal generated by \mathfrak{a} , that is, $\mathfrak{a}_v = \bigcap_{(\alpha) \supseteq \mathfrak{a}} (\alpha)$, (α) running through all fractionary ideals containing \mathfrak{a} . By Krull [6] § 46 this implies that the integrally closed domain R is a Prüfer ring. On the other hand part II of theorem 3 ensures that any finite intersection of principal ideals (more generally of finitely generated ideals) in a Prüfer ring is finitely generated. Then R is both Prüfer and Noetherian, hence a Dedekind domain.

The next criterion for Prüfer rings concerns relations between the quotient of ideals, namely

THEOREM 4. *An integral domain R is a Prüfer ring if and only if one of the following equivalent conditions is satisfied:*

- I. $(\mathfrak{a} + \mathfrak{b}) : \mathfrak{c} = \mathfrak{a} : \mathfrak{c} + \mathfrak{b} : \mathfrak{c}$ for arbitrary ideals \mathfrak{a} and \mathfrak{b} , and finitely generated \mathfrak{c} ;
- II. $\mathfrak{c} : (\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{c} : \mathfrak{a} + \mathfrak{c} : \mathfrak{b}$ for finitely generated \mathfrak{a} and \mathfrak{b} , and arbitrary \mathfrak{c} .

PROOF. For any multiplicative system S in R the relation $(R_S \mathfrak{a} : R_S \mathfrak{b}) = R_S(\mathfrak{a} : \mathfrak{b})$ is easily checked for ideals \mathfrak{a} and \mathfrak{b} in R , provided \mathfrak{b} is finitely generated. Since sums and intersections, as already pointed out, are preserved by passage to quotient ring, the properties I and II follow for

a Prüfer ring by considering the local rings $R_{\mathfrak{p}}$ for maximal \mathfrak{p} where I and II clearly are satisfied, because $R_{\mathfrak{p}}$'s ideals are totally ordered by set inclusion.

By the proof of the remainder of the theorem we shall be utilizing the following lemma which actually in a slightly disguised form appears already by Dedekind [2]:

LEMMA 3. *The integral domain R is a Prüfer ring, if any non-zero ideal, generated by two elements, is invertible.*

A detailed proof may be found in Jaffard [5].

To conclude the proof of theorem 4 let us suppose that I holds. For any two non-zero elements a and b in R property I implies by setting $\mathfrak{a} = (a)$, $\mathfrak{b} = (b)$, $\mathfrak{c} = (a, b)$ that

$$(*) \quad R = (1) = (a) : (b) + (b) : (a) .$$

Hence there exists an element $x \in (a) : (b)$ and $y \in (b) : (a)$ such that $1 = x + y$. Since $ab \mid b(bx)$ and $ab \mid a(ay)$ the relation

$$ab = a(bx) + b(ay)$$

shows that $(a, b) \cdot (bx, ay) = (ab)$, that is, (a, b) is invertible.

Similarly, if II holds good, we obtain (*) by putting

$$\mathfrak{a} = (a), \quad \mathfrak{b} = (b), \quad \mathfrak{c} = (a) \cap (b) ,$$

which as above implies that (a, b) is invertible.

Finally we shall mention and comment on the following well-known theorem (see for instance Jaffard [5]).

THEOREM 5. *The integral domain R is a Prüfer ring if and only if $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{c}$, \mathfrak{a} being a finitely generated ideal $\neq (0)$, implies $\mathfrak{b} = \mathfrak{c}$.*

On this occasion it might be of some interest to notice the following fairly obvious consequence. Recalling that an ideal \mathfrak{a} in the integral domain R is called integrally closed in R 's quotient field K , if any element x in K integrally dependent on \mathfrak{a} , i.e. satisfying an equation of the form

$$x^n + a_1 x^{n-1} + \dots + a_n = 0, \quad a_i \in \mathfrak{a}^i, \quad 1 \leq i \leq n ,$$

belongs to \mathfrak{a} , it is easily seen by Jaffard [5] (corollaire 1, p. 43), that the restricted cancellation law expressed in the above theorem is equivalent to the condition that any finitely generated ideal be integrally closed. Moreover, since any ideal in a Prüfer ring is integrally closed, theorem 5 immediately yields

COROLLARY. *The integral domain R is a Prüfer ring, if and only if any ideal in R is integrally closed in R 's quotient field.*

In connection with theorem 5 the question naturally arises for which rings the unrestricted cancellation law holds for the multiplicative semigroup of all ideals, that is, for which rings will $ab=ac$, $a \neq (0)$, not necessarily finitely generated, imply $b=c$? One might believe that such a ring must be Noetherian and hence a Dedekind domain. This, however, is disproved by choosing for R the ring of all integers in the infinite algebraic number field obtained by adjoining to the rational number field Q the set of all square roots of rational numbers.

We shall finish this paper by giving some necessary and sufficient conditions for a ring that its ideals satisfy the above cancellation law.

THEOREM 6. *For an integral domain R the following conditions are equivalent:*

I. *The cancellation law holds for the semigroup of R 's non-zero ideals, that is $ab=ac$, $a \neq (0) \Rightarrow b=c$.*

II. *R is a Prüfer ring for which any proper prime ideal \mathfrak{p} is maximal and satisfies the condition $\mathfrak{p}^2 \neq \mathfrak{p}$.*

III. *For any maximal ideal \mathfrak{p} in R the quotient ring $R_{\mathfrak{p}}$ is a discrete valuation ring.*

IV. *The semigroup of R 's non-zero ideals may be embedded in a direct product of ordered cyclic groups.*

V. *Any quasi-primary ideal (i.e. the radical being a prime ideal) is irreducible, and $\bigcap_{n=1}^{\infty} \alpha^n = (0)$ for any ideal $\alpha \neq R$.*

VI. *R is a Prüfer ring for which $\bigcap_{n=1}^{\infty} \alpha^n = (0)$ for any ideal $\alpha \neq R$.*

PROOF. We carry out the proof in the following steps: I \Rightarrow II \Rightarrow III \Rightarrow IV \Rightarrow I, III \Rightarrow V \Rightarrow II and III \Leftrightarrow VI.

I \Rightarrow II: That a ring with the property I is a Prüfer ring follows from theorem 5, and the relation $\mathfrak{p}^2 \neq \mathfrak{p}$ clearly is a consequence of the cancellation law. If the second condition in II were not fulfilled there would exist a prime ideal $\mathfrak{q} \neq (0)$ and a maximal ideal \mathfrak{p}^* for which $\mathfrak{q} \subset \mathfrak{p}^*$. From this we shall derive a contradiction by proving that this would imply the relation $\mathfrak{q}\mathfrak{p}^* = \mathfrak{q}$. This is done by showing the relation "locally", i.e. by showing $R_{\mathfrak{p}}(\mathfrak{q}\mathfrak{p}^*) = R_{\mathfrak{p}}\mathfrak{q}$ for any maximal ideal \mathfrak{p} . We have to distinguish the cases $\mathfrak{p} \neq \mathfrak{p}^*$ and $\mathfrak{p} = \mathfrak{p}^*$. For $\mathfrak{p} \neq \mathfrak{p}^*$ the relation follows from $R_{\mathfrak{p}}\mathfrak{p}^* = R_{\mathfrak{p}}$ so that

$$R_{\mathfrak{p}}(\mathfrak{q}\mathfrak{p}^*) = R_{\mathfrak{p}}\mathfrak{q} \cdot R_{\mathfrak{p}}\mathfrak{p}^* = R_{\mathfrak{p}}\mathfrak{q}.$$

For $\mathfrak{p} = \mathfrak{p}^*$ we take into account that $R_{\mathfrak{p}}$ is a valuation ring, R being a

Prüfer ring. Let q be an arbitrary element in $R_p \setminus \mathfrak{p}$ and p some element belonging to $R_p \setminus \mathfrak{p}$ but not to $R_p \setminus \mathfrak{q}$. Since $q \nmid p$, and R_p is a valuation ring we must have $p \mid q$, and therefore we can find an $r \in R_p$ for which $q = pr$. Because $pr \in R_p \setminus \mathfrak{q}$, $p \notin R_p \setminus \mathfrak{q}$ and R_p is a prime ideal, $R_p \setminus \mathfrak{q}$ must contain r . Hence

$$R_p \setminus \mathfrak{q} \subseteq R_p \setminus \mathfrak{p} \cdot R_p \setminus \mathfrak{q} = R_p \setminus (\mathfrak{q}p^*)$$

which together with the trivial converse inclusion shows the desired relation.

II \Rightarrow III. Since R is a Prüfer ring R_p is a valuation ring for maximal \mathfrak{p} . Moreover, on account of the additional assumption on R 's prime ideals, R_p (as a valuation ring) must have rank 1 and be discrete.

III \Rightarrow IV. This implication follows from the fact that the ideals of R are uniquely determined by their local components, and the group of divisibility for R_p is a cyclic ordered group.

IV \Rightarrow I. Obvious.

III \Rightarrow V. Since any proper prime ideal in an integral domain satisfying III clearly must be maximal, we first just have to prove that any primary ideal in R is irreducible. Let \mathfrak{a} be a primary ideal $\neq (0)$ with $\text{Rad } \mathfrak{a} = \mathfrak{p}'$. Suppose we have a decomposition $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$; the ideals of R_p , being totally ordered by set inclusion, the relation

$$R_p \setminus \mathfrak{a} = R_p \setminus \mathfrak{b} \cap R_p \setminus \mathfrak{c}$$

involves $aR_p = bR_p$, say. Since $aR_p = bR_p (= R_p)$ for any $\mathfrak{p} \neq \mathfrak{p}'$, we see that $\mathfrak{a} = \mathfrak{b}$.

The proof of the second assertion $\bigcap_{n=1}^{\infty} \mathfrak{a}^n = (0)$ for $\mathfrak{a} \neq R$ is done indirectly. Assume, there existed an ideal $\mathfrak{b} \neq (0)$ such that $\mathfrak{b} \subseteq \mathfrak{a}^n$ for all n ; we choose a maximal ideal $\mathfrak{p} \supseteq \mathfrak{a}$ and passing to the local ring R_p we get

$$(0) \neq R_p \setminus \mathfrak{b} \subseteq (R_p \setminus \mathfrak{a})^n \subseteq (R_p \setminus \mathfrak{p})^n$$

for all natural numbers n , contradicting the fact that R_p is a discrete valuation ring.

V \Rightarrow II. We first show that any proper prime ideal \mathfrak{p} is maximal. In fact, suppose there existed prime ideals \mathfrak{p} and \mathfrak{q} so that $(0) < \mathfrak{q} < \mathfrak{p} < R$. For any positive integer n $\mathfrak{p}^n \cap \mathfrak{q}$ is quasi-primary, since $\text{Rad}(\mathfrak{p}^n \cap \mathfrak{q}) = \mathfrak{q}$ and hence irreducible. The inclusion $\mathfrak{p}^n \subseteq \mathfrak{q}$ obviously being impossible we must have $\mathfrak{q} \subseteq \mathfrak{p}^n$.

This holds for all n and therefore $(0) \neq \mathfrak{q} \subseteq \bigcap_{n=1}^{\infty} \mathfrak{p}^n$ contrary to the second assumption in V. Since $\mathfrak{p}^2 \neq \mathfrak{p}$ is an immediate consequence of $\bigcap_{n=1}^{\infty} \mathfrak{p}^n = (0)$, it only remains to be shown that R is a Prüfer ring. Since any proper prime ideal \mathfrak{p} is maximal, there is a 1-1 correspondence (preserving set inclusion) between the \mathfrak{p} -primary ideals in R and the

proper ideals in R_p . Now, the p -primary ideals are totally ordered by set inclusion, all of them being irreducible. This involves that R_p is a valuation ring and R therefore a Prüfer ring.

III \Leftrightarrow VI. To establish this equivalence we just have to remark that the valuation ring R_p is discrete if and only if $\bigcap_{n=1}^{\infty} (R_p \mathfrak{p})^n = (0)$.

One final remark. Considering the well-known three axioms for a Dedekind domain R ,

- a) R is Noetherian,
- b) any proper prime ideal is maximal,
- c) R is integrally closed,

together with the obvious fact that R is a Dedekind domain if and only if R is Noetherian and Prüfer, one might think there were some connection between Prüfer rings and domains with the properties b) and c). However, apart from the almost trivial statement that a Prüfer ring necessarily is integrally closed no such connection exists. Choosing for R a valuation ring of rank > 1 we see that b) need not be fulfilled for a Prüfer ring. Furthermore, Krull [7] has given an example of an integrally closed local domain with exactly one non-zero prime ideal, which is not a valuation ring, and thus made clear that the conditions b) and c) do not ensure that R is a Prüfer ring.

ADDED IN PROOF. After this paper has been printed, it has come to my notice, that theorem 2 is in substance a consequence of a result (obtained by other methods) in K. Asano, *Über kommutative Ringe, in denen jedes Ideal als Produkt von Primidealen darstellbar ist*, J. Math. Soc. Japan 3 (1951), 82–90.

REFERENCES

1. I. S. Cohen, *Commutative rings with restricted minimum condition*, Duke Math. J. 17 (1950), 27–42.
2. R. Dedekind, *Über die Begründung der Idealtheorie*, Nachr. Ges. Wiss. Göttingen 1895, 106–113.
3. L. Fuchs, *Über die Ideale arithmetischer Ringe*, Comment. Math. Helv. 23 (1949), 334–341.
4. A. Hattori, *On Prüfer rings*, J. Math. Soc. Japan 9 (1957), 381–385.
5. P. Jaffard, *Les systèmes d'idéaux*, Paris, 1960.
6. W. Krull, *Idealtheorie*, Ergebnisse d. Math. IV₃, Berlin, 1935.
7. W. Krull, *Beiträge zur Arithmetik kommutativer Integritätsbereiche*, Math. Z. 41 (1936), 665–679.