Internat. J. Math. & Math. Sci.
Vol. 9 No. 4 (1986) 749-752

THE GCD PROPERTY AND IRREDUCIBLE QUADRATIC POLYNOMIALS

SAROJ MALIK

D-80, Malvija Nagar
New Delhi, 110017 India

JOE L. MOTT

Department of Mathematics
Florida State University
Tallahassee, FL 32306-3027 U.S.A.

MUHAMMAD ZAFRULLAH

Department of Mathematics
Faculty of Science
Al-Faateh University
Tripoli, Libyan Arab Jamahiriya

(Received April 13, 1984 and in revised form July 3, 1986)

ABSTRACT. The proof of the following theorem is presented: If D is, respectively, a Krull domain, a Dedekind domain, or a Prüfer domain, then D is correspondingly a UFD, a PID, or a Bezout domain if and only if every irreducible quadratic polynomial in $D[X]$ is a prime element.

KEY WORDS AND PHRASES. Prüfer v-multiplication domain, v-operation, v-ideals, Krull domains, Dedekind domains, Prüfer domains, invertible ideals.
1980 MATHEMATICS SUBJECT CLASSIFICATION CODES: 13A15 13F05 13F15

1. PRELIMINARIES

Throughout this note let D, K and X denote respectively an integral domain, its quotient field, and an indeterminate over D.

As a consequence of the considerations of this note we obtain the following results.

Let D be a Krull (Dedekind, Prüfer) domain. Then D is a UFD (PID, or a Bezout domain) if and only if every irreducible quadratic polynomial in $D[X]$ is a prime element.

These results are all corollaries to the following theorem.

THEOREM 1. Let D be a Prüfer v-multiplication domain such that for each pair a,b of elements of $D-\{0\}$, $((a) \cap (b))^{-1} = (c,d)^{-1}$ for some $c,d \in D$. If each irreducible quadratic polynomial in $D[X]$ is a prime, then D is a GCD domain. Conversely, if D is a GCD domain, then $D[X]$ is a GCD domain and each irreducible polynomial over $D[X]$ is a prime.

The proof of Theorem 1 and its corollaries require the notions of v-operation and Prüfer v-multiplication domains. For details on these notions the reader may consult sections 32 and 34 of Gilmer [1]. Nevertheless, we recall the basic definitions.

DEFINITION 1. Let $F(D)$ denote the set of fractional ideals of D. The operation on $F(D)$ defined by $A \to (A^{-1})^{-1} = A_v$, where A ranges over $F(D)$, is called the v-operation. A fractional ideal $A \in F(D)$ is called a v-ideal if $A = A_v$ and a v-ideal A is said to be a v-ideal of finite type if $A = B_v$ where B is a finitely generated fractional ideal. In particular, a v-ideal A is said to be of type 2 if $A = (a,b)_v$ for some pair of elements a and b of K.

We make considerable use of the following basic properties of the v-operation:

For $A,B \in F(D)$

(i) $(A_v)_v = A_v$.

(ii) $(AB)_v = (A_vB)_v = (A_vB_v)_v$.

(iii) If A is a principal fractional ideal, then $(AB)_v = AB_v$.
In particular a principal fractional ideal is a v-ideal.

(iv) $A^{-1} = (A_v)^{-1}$; $D^{-1} = D$, $D_v = D$.

(v) If A and B are v-ideals then $A \cap B$ is a v-ideal.

DEFINITION 2. An integral domain D is called a Prüfer v-multiplication domain (or a PVMD for short) if for each v-ideal A of finite type there is a v-ideal B of finite type such that $(AB)_v = (A_vB)_v = (A_vB_v)_v = D$.

Krull domains, GCD domains, Prüfer domains and their special cases are all Prüfer v-multiplication domains. Among many other things a PVMD is integrally closed.

If $f(X)$ is a polynomial in $K[X]$, then the content of f is the fractional ideal of D generated by the coefficients of $f(X)$. Moreover, we usually denote the content of f by A_f.

In the proof of Theorem 1 we shall also need the following version of Gauss' Lemma (see Proposition 34.8 in [1]):

Let D be integrally closed. If $f,g \in K[X]$ then $(A_{fg})_v = (A_fA_g)_v)$.

It is well known that an integral domain D is a GCD domain if and only if for each pair a,b of elements of D the ideal $(a,b)_v$ is principal. We shall use this fact to prove our theorem; but first a technical lemma.

LEMMA 3. Let D be a PVMD and let $a,b \in D$ then the following statements are equivalent.

(1). There exist $c,d \in D$ such that $((a) \cap (b))^{-1} = (c,d)^{-1}$.

(2). There exist $c,d \in D$ such that $(a) \cap (b) = (c,d)_v$.

(3). There exist $u,v \in K$ such that $((a,b)(u,v))_v = D$.

PROOF. clearly (1)$\Leftrightarrow$(2) so we only prove (2)$\Leftrightarrow$(3). According to Griffin [2] since D is a PVMD, $((a,b)(a) \cap (b))_v = abD$ for each pair a,b of elements of D. Thus $((a,b)((a) \cap (b))/ab)_v = D$. Now let X be a fractional ideal such that $(X(a,b))_v = D$ then $X((a,b)\ ((a) \cap (b))/ab)_v = XD$ and $(X(a,b)\ ((a) \cap (b))/ab)_v = (XD)_v = X_v$. But

$$(X(a,b)((a) \cap (b))/ab)_v = (((X(a,b))_v((a) \cap (b))/ab)_v)_v$$
$$= (D((a) \cap (b))/ab)_v = ((a) \cap (b))/ab .$$

So that $X_v = ((a) \cap (b))/ab$ and hence $((a) \cap (b))/ab$ is of type 2 if and only if X_v is of type 2. This verifies the required equivalence.

2. PROOF OF THE MAIN THEOREM.

We are prepared now to prove Theorem 1. Suppose that D is a PVMD, let $a,b \in D$, and let $c,d \in K$ such that $((a,b)(c,d))_v = D$. We may assume that $(a,b) = A_{(aX+b)}$ and $(c,d) = A_{(cX+d)}$. Thus, we have $(A_{(aX+b)}A_{(cX+d)})_v = D$. Since D is integrally closed, Proposition 34.8 of [1] implies $D = (A_{(aX+b)}A_{(cX+d)})_v = (A_{(aX+b)(cX+d)})_v$. But since $((a,b)(c,d))_v = D$, we conclude $(a,b)(c,d) \subseteq D$. Therefore, $ac, ad, bc, bd \in D$, and $g(X) = (aX+b)(cX+d)$ is a polynomial of degree 2 over $D[X]$. Obviously $g(X)$ is reducible in $D[X]$ since otherwise the hypothesis of the theorem would require $g(X)$ to be prime in $D[X]$ and hence irreducible in $K[X]$. Thus, $g(X)$ is a product of two linear polynomials over $D[X]$, say $g(X) = (rX+s)(tX+u)$ where $r, s, t, u \in D$. Now $(A_{g(X)})_v = D = (A_{rX+s)(tX+u)})_v = (A_{rX+s}A_{(tX+u)})_v = ((r,s)(t,u))_v$. Now as we have already observed in the proof of Lemma 3, $(t,u)_v = ((r) \cap (s))/rs$. But since $t,u \in D$, $((r) \cap (s))/rs \subseteq D$ or, in other words, $(r) \cap (s) \subseteq rsD$. Whence $(r) \cap (s) = rsD$ and $(t,u)_v = ((r) \cap (s))/rs = D$. Similarly $(r,s)_v = D$.

Now since $(aX+b)(cX+d) = (rX+s)(tX+u)$, $aX+b$ is an associate of $rX+s$ or of $tX+u$ in $K[X]$. Say $aX+b = k(rX+s)$. Then $A_{(aX+b)} = A_{k(rX+s)} = kA_{(rX+s)}$ and $(A_{(aX+b)})_v = k(A_{rX+s}))_v = kD$. Thus, we conclude $(a,b)_v = kD$ is a principal ideal.

Since the converse of this theorem is obvious, the proof of theorem 1 is complete.

3. APPLICATIONS OF THE MAIN THEOREM.

We shall now point out some of the known PVMD's which satisfy the requirement that $aD \cap bD = (c,d)_v$. (In what follows we shall call this condition the <u>type two condition</u>.)

(1). Prüfer domains: Recall that D is a Prüfer domain if each finitely generated (fractional) ideal A of D is invertible. It is easy to see that a PVMD is a generalization of a Prüfer domain. That a Prufer domain satisfies the type two condition can be verified from Gilmer and Heinzer [3, p. 143].

(2). Rings of Krull type: A ring of Krull type is a ring D of finite character whose defining family W of valuations has the property that for each $w \in W$ the

corresponding valuation domain D_w is a quotient ring of D (cf. Griffin [4] for details).

According to [4] a ring of Krull type is a PVMD. In fact a ring of Krull type is a generalization of a Krull domain. Moreover, according to [4] every v-ideal A of finite type of a ring of Krull type is a v-ideal of type two. As a result of the above observation appropriate corollaries can be derived. But since the Krull and Dedekind domains are the more well known special cases of the above mentioned type two PVMD's we state the following corollary.

COROLLARY 4. A Krull (Dedekind) domain is a UFD (PID) if and only if each irreducible quadratic polynomial over D is a prime.

REMARK 5. The obvious analogue of Corollary 4 for Prüfer domains can be found, implicitly, in the proof of part (b) of Theorem 28.8 of [1].

REMARK 6. The conditions under which a Krull domain becomes a UFD have always been of interest and Corollary 4 gives probably the simplest such condition.

REMARK 7. Since the class of Prüfer v-multiplication domains contain the class of Prüfer domains it seems reasonable to conjecture that for each pair of elements of a PVMD, $aD \cap bD$ is a v-ideal of type 2. At this time we have not been able to prove or disprove this conjecture.

REMARK 8. From the proof of Theorem 1 it follows that this theorem can be stated in the following alternative form.

Let D be a PVMD with the type two property. If each irreducible quadratic polynomial of $D[X]$ is irreducible in $K[X]$, then D is a GCD domain. Conversely, if D is a GCD domain, then each irreducible polynomial of $D[X]$ is a prime.

As a consequence of the above stated form of Theorem 1, we can say that if D is a PVMD with type two property such that D is not a GCD domain then there must exist a quadratic polynomial in $D[X]$, which is irreducible over $D[X]$ and reducible over $K[X]$.

REFERENCES

1. GILMER, R. Multiplicative Ideal Theory, Marcel Dekker, New York, 1972.

2. GRIFFIN, M. Some Results on v-Multiplication Rings, Canad. J. Math. 19 (1967), 710-722.

3. GILMER, R. and HEINZER, W. On the Number of Generators of an Invertible Ideal, J. Alg. 14, 2 (1970), 139-151.

4. GRIFFIN, M. Rings of Krull Type, J. Reine Angew. Math. 229 (1968), 1-27.