PROPERTIES OF SOME CLASSICAL INTEGRAL DOMAINS

THESIS

Presented to the Graduate Council of the
North Texas State University in Partial
Fulfillment of the Requirements

For the Degree of

MASTER OF SCIENCE

By

Timothy B. Crawford, B. A.
Denton, Texas
May, 1975

M.S.

Crawford, Timothy B., Properties of Some Classical Integral Domains. Master of Science (Mathematics), May, 1975, 35 pp., bibliography, 1 title.

Greatest common divisor domains, Bezout domains, valuation rings, and Prüfer domains are studied. Chapter One gives a brief introduction, statements of definitions, and statements of theorems without proof. In Chapter Two theorems about greatest common divisor domains and characterizations of Bezout domains, valuation rings, and Prüfer domains are proved. Also included are characterizations of a flat overring. Some of the results are that an integral domain is a Prüfer domain if and only if every overring is flat and that every overring of a Prüfer domain is a Prüfer domain.

TABLE OF CONTENTS

CHAPTER I

Introduction

The purpose of this paper is to investigate and characterize several of the classical integral domains. Included are greatest common divisor domains, valuation rings, Bezout domains, and Prüfer domains. A basic knowledge of commutative ring theory is assumed in the paper.

Before stating the definitions and theorems, a remark on notation is in order. D will represent an integral domain with multiplicative identity different from the additive identity and quotient field K.

Several definitions and theorems used in this paper will now be listed. Proofs of the theorems can be found in Zariski and Samuel, Vol. 1, 1958.

<u>Theorem 1.1</u>: If R is a commutative ring with a unity, and A is an ideal of R such that $A \neq R$, then A is contained in a maximal ideal of R.

<u>Definition 1.1</u>: If $a, b \in D$, then a <u>divides</u> b, denoted by $a|b$, if and only if there exists $c \in D$ such that $a \cdot c = b$.

<u>Definition 1.2</u>: If $a, b, d \in D$, then d is a <u>greatest common divisor</u> of a and b, denoted by $(a,b) = d$, if and only if

(i) $d|a$ and $d|b$, and

(ii) if $d_1 \in D$ such that $d_1|a$ and $d_1|b$, then $d_1|d$.

Definition 1.3: An integral domain D is a greatest common divisor domain, $\mathcal{G.C.D.}$ domain, if and only if every pair (and hence every finite number) of non-zero elements has a greatest common divisor.

Definition 1.4: If a, b, m $\in$ D, then m is a least common multiple of a and b if and only if

(i) $a|m$ and $b|m$, and

(ii) if $m_1 \in D$ such that $a|m_1$ and $b|m_1$, then $m|m_1$.

Definition 1.5: An integral domain D is a least common multiple domain if and only if every pair (and hence every finite number) of non-zero elements has a least common multiple.

Theorem 1.2: D is a $\mathcal{G.C.D.}$ domain if and only if D is a least common multiple domain.

Theorem 1.3: Every unique factorization domain is a $\mathcal{G.C.D.}$ domain.

Definition 1.6: If $D \subset J \subset K$ and A is an ideal in D and A' is an ideal in J, then $A^e = A \cdot J$ and $A'^c = A' \cap D$. A^e is called the extension of A to J and A'^c is called the contraction of A' to D.

Definition 1.7: If P is a proper prime ideal of D, then $D_P = \{\frac{r}{s} | r, s \in D, s \notin P\}$.

Theorem 1.4: If $D \subset J \subset K$ and A and B are ideals in D and A' and B' are ideals in J, then the following are true.

(a) (i) If $A \subset B$, then $A^e \subset B^e$.

(ii) If $A' \subset B'$, then $A'^c \subset B'^c$.

(b) (i) $(A'^{c})^{e} \subset A'$,

(ii) $A \subset (A^{e})^{c}$.

(c) (i) $[(A'^{c})^{e}]^{c} = A'^{c}$,

(ii) $A^{e} = [(A^{e})^{c}]^{e}$

(d) (i) $(A' + B')_{c} \supset A'^{c} + B'^{c}$

(ii) $(A + B)^{e} = A^{e} + B^{e}$

(e) (i) $(A' \cap B')^{c} = A'^{c} \cap B'^{c}$

(ii) $(A \cap B)^{e} \subset A^{e} \cap B^{e}$

(iii) if $J = D_{p}$ for some proper prime ideal P of D, then $(A \cap B)^{e} = A^{e} \cap B^{e}$.

(f) (i) $(A' \ B')^{c} \supset (A'^{c}) \cdot (B'^{c})$

(ii) $(A \cdot B)^{e} = A^{e} \cdot B^{e}$

(g) (i) $(A' : B')^{c} \subset (A'^{c}) : (B'^{c})$

(ii) $(A:B)^{e} \subset A^{e} : B^{e}$

(h) (i) $(\sqrt{A'})^{c} = \sqrt{A'^{c}}$

(ii) $(\sqrt{A})^{e} \subset \sqrt{A^{e}}$.

Definition 1.8: A non-empty subset N of K is a fractional ideal of D if and only if

(i) if $x, y \in N$, then $x - y \in N$,

(ii) if $r \in D$ and $x \in N$, then $rx \in N$, and

(iii) there exists an element $0 \neq d \in D$ such that $N \subset \frac{1}{d} D$, i.e., $dN \subset D$.

Theorem 1.5: If N is a fractional ideal of D and $d \in D$ such that $dN \subset D$, then dN is an ideal of D.

Theorem 1.6: If M and N are fractional ideals of D, then $N + M$, $N \cdot M$, $N \cap M$, and $N:M$ are fractional ideals of D.

Definition 1.9: D is a valuation ring if and only if for every $x \in K$, either $x \in D$ or $x^{-1} \in D$.

Definition 1.10: D is quasi-local if and only if there exists a unique maximal ideal of D.

Theorem 1.7: If $D \subset D' \subset K$, then D' is a valuation ring, every non-unit in D' is in D, and if M' is the maximal ideal of D', then M' is a prime ideal of D and $D' = D_{M'}$.

Theorem 1.8: If P is a proper prime ideal of D, then D_P is quasi-local with maximal ideal PD_P and $PD_P \cap D = P$.

Theorem 1.9: If A is a proper ideal of D and $\alpha \in K$ such that $\alpha \neq 0$, then $1 \notin A \cdot D[\alpha]$ or $1 \notin A \cdot D[\alpha^{-1}]$.

CHAPTER II

PROPERTIES OF SOME CLASSICAL INTEGRAL DOMAINS

<u>Theorem 2.1</u>: Let D be a $\mathscr{G}.\mathscr{C}.\mathscr{D}.$ domain and let a, b $\in$ D such that $(a,b) = d$ where $a = \alpha d$ and $b = \beta d$, then $(\alpha,\beta) = 1$.

<u>Proof</u>: Suppose that $(\alpha,\beta) = h$. We show $h|1$. Now we know that $h|\alpha$ and $h|\beta$ which implies that $hw_1 = \alpha$ and $hw_2 = \beta$ for some w_1, $w_2 \in D$. This implies that $a = \alpha d = hdw_1$ and $b = \beta d = hdw_2$. Therefore $hd|a$ and $hd|b$ which implies $hd|d$ or $h\cdot d\cdot k = d$ for some $k \in D$. This implies that $h\cdot k = 1$ or $h|1$. Hence $(\alpha,\beta) = 1$.

<u>Theorem 2.2</u>: Let D be a $\mathscr{G}.\mathscr{C}.\mathscr{D}.$ domain and let a, b $\in$ D such that $(a,b) = d$, then $(ka, kb) = kd$ for any $k \in D$.

<u>Proof</u>: Since $(a,b) = d$, then $a = \alpha d$ and $b = \beta d$ where $\alpha, \beta \in D$ and $(\alpha,\beta) = 1$. This implies that $ka = \alpha\cdot kd$ and $kb = \beta\cdot kd$ or $kd|ka$ and $kd|kb$. Suppose $(ka, kb) = d'$, but since $kd|ka$ and $kd|kb$, then $kd|d'$ which implies $kd\,w = d'$. This implies $kdw|kd\alpha$ and $kdw|kd\beta$ which implies $w|\alpha$ and $w|\beta$. Therefore $w|(\alpha,\beta)$ or $w|1$. Hence $w\cdot w_1 = 1$ and since $kdw = d'$ then $kd\cdot w\cdot w_1 = d'\cdot w_1$ or $kd = d'\cdot w_1$ which implies $d'|kd$ and then $(ka, kb) = kd$.

<u>Theorem 2.3</u>: Let D be a $\mathscr{G}.\mathscr{C}.\mathscr{D}.$ domain and a, b $\in$ D such that $(a,b) = 1$. If $a|bc$, then $a|c$.

Proof: Since $(a,b) = 1$, then from Theorem 2.2, $(ac,bc) = c$. But now $a|ac$ and $a|bc$ which implies $a|c$.

Theorem 2.4: If D is a $\mathscr{G}.\mathscr{C}.\mathscr{D}.$ domain and $a, b \in D$ such that $(a,b) = 1$, then $(a, b^n) = 1$ for every $n \in I^+$.

Proof: We use induction. The theorem is true clearly for $n = 1$. Suppose the theorem true for $n = k$. We show $(a,b^{k+1}) = 1$. Since $(a,b^k) = 1$, then $(a^2b,ab^{k+1}) = ab$ from Theorem 2.2. Suppose $(a,b^{k+1}) = d$. Then $(a^2,ab^{k+1}) = ad$ and since $ad|a^2$, then $ad|a^2b$ and $ad|ab^{k+1}$ which implies $ad|ab$ or $d|b$. But now $d|a$ and $d|b$ which implies $d|1$. Hence $(a,b^{k+1}) = 1$ and induction is complete.

Theorem 2.5: If D is an integral domain and $a, b \in D$ such that $b|a$, then $b^n|a^n$ for every $n \in I^+$.

Proof: Since $b|a$, we know $b \cdot k_1 = a$ for some $k_1 \in D$. Let $n \in I^+$. Then $(bk_1)^n = a^n$ which implies $b^n \cdot k_1{}^n = a^n$ or $b^n|a^n$.

Theorem 2.6: Let D be a $\mathscr{G}.\mathscr{C}.\mathscr{D}.$ domain with quotient field K. If $u \in K$ such that $u^n + a_{n-1}u^{n-1} + \dots + a_1u + a_0 = 0$ where $a_i \in D$ for every $i \in \{0,1,\dots,n-1\}$, then $u \in D$.

Proof: Since $u \in K$, then $u = \frac{r}{s}$ where $r, s \in D$ and $s \neq 0$. Now D is a $\mathscr{G}.\mathscr{C}.\mathscr{D}.$ domain so there exists $d \in D$ such that $d = (r,s)$. Now $r = \alpha d$ and $s = \beta d$ where $(\alpha,\beta) = 1$. If $r = 0$, the theorem is trivial. So suppose $r \neq 0$. Then $u^n + a_{n-1}u^{n-1} + \dots + a_1u + a_0 = 0$ implies

$$\left(\frac{\alpha d}{\beta d}\right)^n + a_{n-1}\left(\frac{\alpha d}{\beta d}\right)^{n-1} + \dots + a_1\frac{\alpha d}{\beta d} + a_0 = 0$$

which implies

$$\frac{\alpha^n}{\beta^n} + a_{n-1}\frac{\alpha^{n-1}}{\beta^{n-1}} + \dots + a_1\frac{\alpha}{\beta} + a_0 = 0.$$

This implies

$$\alpha^n + a_{n-1}\alpha^{n-1}\beta + \dots + a_1\alpha\beta^{n-1} + a_0\beta^n = 0$$

which implies

$$\alpha^n = \beta(-a_{n-1}\alpha^{n-1} - \dots - a_1\alpha\beta^{n-z} - a_0\beta^{n-1}).$$

This implies $\beta|\alpha^n$ but from Theorem 2.4 since $(\beta,\alpha) = 1$ then $(\beta,\alpha^n) = 1$ for every $n \in I^+$. Now $\beta|\beta$ is clear and $\beta|\alpha^n$ from the above which implies $\beta|1$. Hence β is a unit in D which implies $u = \frac{r}{s} = \frac{\alpha}{\beta} = \alpha\beta^{-1} \in D$.

Theorem 2.7: If D is a $\mathcal{G}.\mathcal{C}.\mathcal{D}.$ domain and $d \in D$ such that $d \neq 0$, and if $f(x)$ is a primitive polynomial in $D[x]$, then $(f(x),d)$ is 1 in D.

Proof: Suppose that $(f(x),d) = d_1 \in D$. Then d_1 divides the coefficients on $f(x)$ and $d_1|d$ which implies $d_1|1$ since $f(x)$ is primitive in $D[x]$, i.e., the greatest common divisor of the coefficients is 1 in D.

Theorem 2.8: Let D be a $\mathcal{G}.\mathcal{C}.\mathcal{D}.$ domain and let $f(x)$ and $g(x)$ be primitive polynomials in $D[x]$. Then $f(x)\cdot g(x)$ is a primitive polynomial in $D[x]$.

Proof: We use induction on the degrees of $f(x)$ and $g(x)$. First we show that if the degree of $f(x)$ is 1 and the degree of $g(x)$ is k then $f(x)\cdot g(x)$ is primitive in $D[x]$. Then we suppose the theorem true for any $f(x)$ of degree less than or equal to p, i.e., if we have any two primitive polynomials in $D[x]$, one of which has degree less than or equal to p, then the product of these two polynomials is primitive in $D[x]$. Then we show the theorem true for $f(x)$ of degree $p + 1$, i.e. if $\deg\{f(x)\} = p + 1$ and $\deg\{g(x)\} = m$, then $f(x)\cdot g(x)$ is primitive in $D[x]$. This will complete the induction and the product of primitives in $D[x]$ will once more be primitive.

Suppose $\deg\{f(x)\} = 1$ and $\deg\{g(x)\} = m$. Then $f(x) = a_0 + a_1x$ and $g(x) = b_o + b_1x + \dots + b_mx^m$. This implies

$$\begin{aligned} f(x)\cdot g(x) &= a_0b_0 + (a_0b_1 + a_1b_0)x + \\ &+ (a_0b_2 + a_1b_1)x^2 + \dots + (a_0b_j + a_1b_{j-1})x^j + \\ &+ \dots + (a_0b_m + a_1b_{m-1})x^m + a_1b_mx^{m+1}. \end{aligned}$$

Suppose d divides each of the coefficients on $f(x)\cdot g(x)$ and let $(d,a_0) = u$. Since $u|a_0$ then $u|a_0b_i$ for every $i \in \{1,\dots,m\}$ which implies that $u|a_1b_i$ for every $i \in \{1,\dots,m\}$ but this implies that u divides $(a_1b_0,\dots,a_1b_m)$ which implies $u|a_1$ but since $u|a_0$ and $u|a_1$ then $u|1$ or u is a unit in D. Therefore $(a_0,d) = 1$ which implies that $d|b_0$ which implies that $d|a_0b_1$ since $d|a_1b_0$ and $d|a_0b_1 + a_1b_0$ but this implies $d|b_1$. This implies that $d|b_2$ since $d|a_1b_1$ and $d|a_0b_2 + a_1b_1$. By an analogous argument $d|b_i$ for $i \in \{1,\dots,m\}$ which implies $d|1$. Hence $f(x)\cdot g(x)$ is a primitive polynomial in $D[x]$.

Now suppose the theorem is true if $\deg\{f(x)\} \le p$ and any $g(x)$, i.e., if $h(x)$ and $k(x)$ are primitive polynomials in D[x], one of which has degree less than or equal to p, then $f(x)\,g(x)$ is primitive in D[x]. Now suppose the degree of f(x) is p + 1 and the degree of g(x) is m. Let us consider f(x) in K[x]. Now either f(x) is prime in K[x] or f(x) is not prime in K[x]. If f(x) is prime in K[x] then f(x) is clearly prime in D[x]. So if $f(x)\cdot g(x) = d\cdot h(x)$ in D[x] then $f(x)|h(x)$ which implies $g(x) = d\cdot g_1(x)$ where $g_1(x) \in D[x]$. This implies that d divides the coefficient of g(x) which implies $d|1$. Hence if f(x) is prime in K[x] then $f(x)\cdot g(x)$ is primitive in D[x]. Now suppose f(x) is not prime in K[x], then $f(x) = f_1(x)\cdot f_2(x)$ where $f_1(x)$ and $f_2(x)$ are both of positive degree, say s and t respectively, such that $s + t = p + 1$. Now

$$f_1(x) = \frac{\alpha_0}{\beta_0} + \dots + \frac{\alpha_s}{\beta_s} x^s$$

and

$$f_2(x) = \frac{\gamma_0}{\delta_0} + \dots + \frac{\gamma_t}{\delta_t} x^t,$$

where $\alpha_i, \beta_i, \gamma_i, \delta_i \in D$ and $\beta_i \neq 0$ and $\delta_i \neq 0$ for every i. Now

$$(\prod_{i=1}^{s} \beta_i)\, f_1(x) \in D[x]$$

and

$$(\prod_{i=1}^{s} \delta_i)\, f_2(x) \in D[x]$$

which implies that

$$(\prod_{i=1}^{s} \beta_i)\, f_1(x) = d_1\cdot f_1'(x)$$

and

$$(\prod_{i=1}^{s} \delta_i)\, f_2(x) = d_2\cdot f_2'(x)$$

where $d_1, d_2 \in D$ and $f_1'(x)$ and $f_2'(x)$ are primitive polynomials in $D[x]$.

Now $f(x)\cdot g(x) = f_1(x)\cdot f_2(x)\cdot g(x)$ which implies that

$$(\prod_{i=1}^{s} \beta_i)(\prod_{i=1}^{t} \delta_i)\ f(x)\cdot g(x) = d_1\cdot d_2\ f_1'(x)\cdot f_2'(x)\cdot g(x).$$

This implies that

$$(\prod_{i=1}^{s} \beta_i)(\prod_{i=1}^{t} \delta_i)\ f(x) = d_1\cdot d_2\cdot f_1'(x)\cdot f_2'(x).$$

Now $f_1'(x)\cdot f_2'(x)$ is primitive by the induction hypothesis which implies that $(\prod_{i=1}^{s} \beta_i)(\prod_{i=1}^{t} \delta_i) = u\cdot d_1\cdot d_2$ where u is a unit in D. Hence

$$f(x)\cdot g(x) = u\cdot f_1'(x)\cdot f_2'(x)\cdot g(x)$$

but now $f_2'(x)\cdot g(x)$ is primitive in $D[x]$ since $\deg\{f_2'(x)\} < p + 1$ and so is $f_1'(x)\cdot(f_2'(x)\ g(x))$ since $\deg\{f_1'(x)\} < p + 1$. Hence $f_1'(x)\cdot f_2'(x)\cdot g(x)$ is primitive in $D[x]$ and so is $u\cdot f_1'(x)\cdot f_2'(x)\cdot g(x)$ since u is a unit in D. This implies that $f(x)\cdot g(x)$ is primitive in $D[x]$and the induction is complete.

<u>Theorem 2.9</u>: If D is a $\mathcal{G.C.D.}$ domain, then $D[x]$ is a $\mathcal{G.C.D.}$ domain.

<u>Proof</u>: Let $f(x), g(x)$ be primitive polynomials in $D[x]$. Note that if $D[x]$ is a $\mathcal{G.C.D.}$ domain with respect to the primitive polynomials in $D[x]$, then any polynomial in $D[x]$can be written as the greatest common divisor of the coefficients

multiplied by a primitive polynomial, and it will then be clear that D[x] is a $\mathcal{G}.\mathcal{C}.\mathcal{D}.$ domain. Consider now f(x), g(x) in K[x]. K[x] is a P.I.D. with a unity and therefore (f(x),g(x)) = (d(x)) in K[x]. Now

$$d(x) = \frac{\alpha_0}{\beta_0} + \frac{\alpha_1}{\beta_1}x + \ldots + \frac{\alpha_n}{\beta_n}x^n$$

where each $\alpha_i, \beta_i \in D$ and $\beta_i \neq 0$. Now $f(x) \in (d(x))$ and $g(x) \in (d(x))$ which implies that $f(x) = d(x) \cdot k_1(x)$ and $g(x) = d(x) \cdot k_2(x)$, where $k_1(x), k_2(x) \in K[x]$. This implies that

$$f(x) = \left(\frac{\alpha_0}{\beta_0} + \frac{\alpha_1}{\beta_1}x + \ldots + \frac{\alpha_n}{\beta_n}x^n\right)$$

$$\cdot\left(\frac{\gamma_0}{\delta_0} + \frac{\gamma_1}{\delta_1}x + \ldots + \frac{\gamma_m}{\delta_m}x^m\right)$$

and

$$g(x) = \left(\frac{\alpha_0}{\beta_0} + \frac{\alpha_1}{\beta_1}x + \ldots + \frac{\alpha_n}{\beta_n}x^n\right)$$

$$\left(\frac{\omega_0}{\eta_0} + \frac{\omega_1}{\eta_1}x + \ldots + \frac{\omega_t}{\eta_t}x^t\right)$$

where $\gamma_i, \delta_i, \omega_i, \eta_i \in D$ and $\delta_i \cdot \eta_i \neq 0$ for any i. We can rationalize the denominator on d(x), $k_1(x)$, $k_2(x)$ and then

$$\prod_{i=0}^{n} \beta_i \cdot d(x) = d_1(x),$$

$$\prod_{i=0}^{m} \delta_i \cdot k_1(x) = r_1(x),$$

$$\prod_{i=0}^{t} \eta_i \cdot k_2(x) = r_2(x).$$

Now $d_1(x)$, $r_1(x)$, and $r_2(x)$ are in D[x] which implies that

$$\left(\prod_{i=0}^{n} \beta_i\right)\left(\prod_{i=0}^{m} \delta_i\right)\cdot f(x) = d_1(x)\cdot r_1(x)$$

and

$$\left(\prod_{i=0}^{n} \beta_i\right)\left(\prod_{i=1}^{n} \eta_i\right)\cdot g(x) = d_1(x)\cdot r_2(x).$$

Let d be the greatest common divisor of the coefficients of $d_1(x)$ so that $d_1(x) = d\cdot d_2(x)$ where $d_2(x)$ is primitive in D[x]. This implies that

$$\left(\prod_{i=0}^{n} \beta_i\right)\left(\prod_{i=0}^{m} \delta_i\right)\cdot f(x) = d\cdot d_2(x)\cdot r_1(x)$$

and

$$\left(\prod_{i=0}^{n} \beta_i\right)\left(\prod_{i=0}^{t} \eta_i\right)\cdot g(x) = d\cdot d_2(x)\cdot r_2(x)$$

but now f(x) and g(x) are primitive which implies that the greatest common divisor of the coefficients of f(x) and d is 1 and also the coefficients of g(x) and d is 1 in D. Hence $d\,|\left(\prod_{i=0}^{n} \beta_i\right)\left(\prod_{i=0}^{m} \delta_i\right)$ and $d\,|\left(\prod_{i=0}^{n} \beta_i\right)\left(\prod_{i=0}^{t} \eta_i\right)$ which implies that $d\cdot w_1 = \left(\prod_{i=0}^{n} \beta_i\right)\left(\prod_{i=0}^{m} \delta_i\right)$ and that $d\cdot w_2 = \left(\prod_{i=0}^{n} \beta_i\right)\left(\prod_{i=0}^{t} \eta_i\right)$ for some $w_1, w_2 \in D$. Hence $w_1\cdot f(x) = d_2(x)\cdot r_1(x)$ and $w_2\cdot g(x) = d_2(x)\cdot r_2(x)$. Now let y_1 and y_2 be the greatest common divisors of the coefficients of $r_1(x)$ and $r_2(x)$, respectively. Then $r_1(x) = y_1u_1(x)$ and $r_2(x) = y_2u_2(x)$ where $u_1(x)$ and $u_2(x)$ are primitive polynomials in D[x]. Therefore $w_1\cdot f(x) = d_2(x)\cdot y_1u_1(x)$ and $w_2\cdot g(x) = d_2(x)\cdot y_2u_2(x)$

which implies that $y_1 | w_1$ and $y_2 | w_2$ but now also $d_2(x) \cdot u_1(x)$ is primitive and $d_2(x) \cdot u_2(x)$ is primitive which implies that $w_1 | y_1$ and $w_2 | y_2$. This implies that $w_1 = u_1 y_1$ and $w_2 = u_2 \cdot y_2$ where u_1 and u_2 are units in D. Hence $u_1 \cdot (f(x) = d_2(x) \cdot u_1(x)$ and $u_2 \cdot g(x) = d_2(x) \cdot u_2(x)$ which implies that

$$f(x) = u_1^{-1} \cdot d(x) \cdot u_1(x)$$

and

$$g(x) = u_2^{-1} \cdot d_2(x) \cdot u_2(x).$$

Therefore $d_2(x) | f(x)$ and $d_2(x) | g(x)$.

Suppose now that there exists $d_3(x) \in D[x]$ such that $d_3(x) | f(x)$ and $d_3(x) | g(x)$. This implies that

$$f(x) = d_3(x) \cdot q_1(x)$$

and

$$g(x) = d_3(x) \cdot q_2(x)$$

where $q_1(x), q_2(x) \in D[x]$. This implies that $(f(x) \subset (d_3(x))$ and $(g(x)) \subset (d_3(x))$ which implies that $(f(x), g(x)) \subset (d_3(x))$. Consider once again $(f(x), g(x))$ in K[x]. This implies $(f(x), g(x)) = (d(x)) \subset (d_3(x))$ in K[x], which implies that $d(x) = d_3(x) \cdot c(x)$ where $c(x) \in K[x]$. This implies that

$$d_1(x) = (\prod_{i=0}^{n} \beta_i) d_3(x) \cdot c(x)$$

which implies that

$$d \cdot d_2(x) = (\prod_{i=0}^{n} \beta_i) \cdot d_2(x) \cdot c(x).$$

Let $c'(x)$ be the rationalized polynomial of $c(x)$ in D[x].

i.e., $c'(x) = k \cdot c(x)$ where k is the product of the denominators of the coefficients of $c(x)$. Let d' be the greatest common divisor of the coefficients on $c'(x)$ so that $c(x) = k \cdot d' \cdot c''(x)$ where $c''(x)$ is a primitive polynomial in $D[x]$. Then

$$d \cdot d_2(x) = \left(\prod_{i=0}^{n} \beta_i\right)(k \cdot d') \cdot d_3(x) \cdot c''(x).$$

But now we claim $d_3(x)$ is primitive in $D[x]$ also. Since $d_3(x) | f(x)$ in $D[x]$ then $d_3(x) \cdot w_1(x) = f(x)$ and if $d_3(x)$ is not primitive then neither is $f(x)$. So $d_3(x)$ is a primitive polynomial in $D[x]$ which implies as before that d and $\left(\prod_{i=0}^{n} \beta_i\right)(k \cdot d')$ are associates. This implies that $v \cdot d = \left(\prod_{i=0}^{n} \beta_i\right)(k \cdot d')$ where v is a unit in D. Hence $d_2(x) = v \cdot d_3(x) \cdot c''(x)$ which implies that $d_3(x) | d_2(x)$, and therefore $D[x]$ is a $\mathcal{S}.\mathcal{C}.\mathcal{D}.$ domain.

Theorem 2.10: Let D be a $\mathcal{S}.\mathcal{C}.\mathcal{D}.$ domain and let P be a prime ideal in $D[x]$ such that $P \cap D = (0)$ in D. Then P is principal.

Proof: Let $f(x) \in P$ such that if $g(x) \in P$ then $\deg f(x) \leq \deg g(x)$. Let $d \in D$ be the greatest common divisor of the coefficients of $f(x)$, then $f(x) = d \cdot f_1(x)$ where $f_1(x)$ is primitive in $D[x]$. We show $P = (f_1(x))$. Now $d \cdot f_1(x) \in P$ implies that $f_1(x) \in P$ since $d \notin P$. Therefore, this implies that $(f_1(x)) \subset P$. Let $g(x) \in P$, then $\deg g(x) \geq \deg f_1(x)$. Suppose $\deg g(x) = \deg f_1(x)$, then if

$$f_1(x) = a_0 + a_1x + \ldots + a_nx^n,$$
$$g(x) = b_0 + b_1x + \ldots + b_nx^n.$$

This implies that $b_nf_1(x) - a_ng(x) \in P$ of degree n-1, which implies that $b_nf_1(x) = a_ng(x) = 0$ which implies that $b_nf_1(x) = a_ng(x)$ but now $(a_n, f_1(x)) = 1$ which implies that $a_n | b_n$ or $a_n \cdot k = b_n$. Hence $k\, f_1(x) = g(x)$ which implies $g(x) \in (f_1(x))$. Suppose that $\deg g(x) > \deg f_1(x)$. Let $d(x) = (g(x), f_1(x))$, then $d(x) \cdot k_1(x) = g(x)$ and $d(x) \cdot k_2(x) = f_1(x)$, where $k_1(x), k_2(x) \in D[x]$. Suppose $\deg d(x) = 0$, then $d(x) = d \in D$ and if $d | f_1(x)$ then $d | 1$ which implies d is a unit in D. This implies that $(f_1(x), g(x)) = 1$. Consider the ideal $(f_1(x), g(x))$ in $K[x]$. Since $(f_1(x), g(x)) = 1$ in $D[x]$, then $(f_1(x), g(x)) = (1)$ in $K[x]$ since $K[x]$ is a P.I.D. with a unity. Hence there exists $r_1(x), r_2(x) \in K[x]$ such that $1 = r_1(x) \cdot f_1(x) + r_2(x) \cdot g(x)$. By rationalizing the denominators on the coefficients of $r_1(x)$ and $r_2(x)$, we get

$$d = r_1'(x) \cdot f_1(x) + r_2'(x) \cdot g(x)$$

where $r_1'(x), r_2'(x) \in D[x]$. This implies that

$$d \in (f_1(x), g(x)) \subset P \text{ in } D[x]$$

which is a contradiction since $P \cap D = (0)$ in D. Hence $\deg d(x) \neq 0$. This implies $1 \leq \deg d(x) \leq n$ which implies that $g(x) = d(x) \cdot k_1(x)$ and $f_1(x) = d(x) \cdot k_2(x)$ where the degrees of

$d(x), k_1(x), k_2(x)$ are all positive. Suppose $\deg d(x) \neq n$. Then $\deg d(x) < n$ and $\deg k_2(x) < n$ which implies $d(x) \notin P$ and $k_2(x) \notin P$ but this implies that $f_1(x) \notin P$ which is a contradiction since $f_1(x) \in P$. Therefore $\deg d(x) = n$ which implies that $\deg k_2(x) = 0$. Therefore $k_2(x) = k \in D$ and $f_1(x) = d(x) \cdot k$ but now $f_1(x)$ is primitive which implies that k is a unit in D. Hence $f_1(x) \cdot k^{-1} = d(x)$ and since $g(x) = d(x) \cdot k_1(x)$ then $g(x) = f_1(x) \cdot k^{-1} \cdot k_1(x)$ which implies $g(x) \in (f_1(x))$. Hence $P \subset (f_1(x))$ and $P = (f_1(x))$.

Theorem 2.11: The following are equivalent.

(a.) D is a valuation ring.

(b.) If A and B are ideals in D, then either $A \subset B$ or $B \subset A$.

(c.) If (a) and (b) are principal ideals in D, then either $(a) \subset (b)$ or $(b) \subset (a)$.

Proof: (a.) implies (b.) Let A and B be ideals in D. Suppose, to the contrary, that $A \not\subset B$ and $B \not\subset A$. This implies that there exists $x \in A$ such that $x \notin B$, and there exists $y \in B$ such that $y \notin A$. Now $\frac{x}{y} \in K$, which implies $\frac{x}{y} \in D$ or $\frac{y}{x} \in D$. Suppose $\frac{x}{y} \in D$, then $\frac{x}{y} \cdot y \in B$ which implies $x \in B$ which is a contradiction to the supposition that $x \notin B$. Suppose now that $\frac{y}{x} \in D$. This implies that $\frac{y}{x} \cdot x \in A$ which implies $y \in A$ which is a contradiction to the supposition that $y \notin A$. Hence either $A \subset B$ or $B \subset A$. (b.) implies (c.) Let (a) and (b) be principal ideals in D. Then (a) and (b) are ideals in D and from (b.) either $(a)\subset(b)$ or $(b)\subset(a)$. (c.) implies (a.). Let $x \in K$. Then $x = \frac{\alpha}{\beta}$ where $\alpha, \beta \in D$. From (c.) we know that either $(\alpha)\subset(\beta)$ or $(\beta)\subset(\alpha)$. Suppose $(\alpha)\subset(\beta)$. This implies that $\alpha \in (\beta)$ which implies $\alpha = d\cdot\beta$ where $d \in D$. But then $\frac{\alpha}{\beta} = d$ which implies $\frac{\alpha}{\beta} \in D$. Suppose $(\beta)\subset(\alpha)$. This implies $\beta \in (\alpha)$ which implies $\beta = d_1\cdot\alpha$ where $d_1 \in D$. But then $\frac{\beta}{\alpha} = d_1$ which implies $\frac{\beta}{\alpha} \in D$. Hence either $x \in D$ or $x^{-1} \in D$, and D is a valuation ring.

Definition 2.1: An integral domain D is a Bezout domain iff every finitely generated ideal of D is principal.

Theorem 2.12: An integral domain D is a Bezout domain iff D is a $\mathcal{G.C.D.}$ domain and D_P is a valuation ring for every proper prime ideal P of D.

Proof: Suppose D is a Bezout domain. Let $a,b \in D$, then $(a,b) = (d)$ for some $d \in D$. We show d is the greatest common divisor of a and b. Since $(a,b) = (d)$, then $a \in (d)$ and $b \in (d)$ which implies $a = r_1 d$ and $b = r_2 d$ where $r_1, r_2 \in D$. This implies that $d|a$ and $d|b$. Suppose there exists an element $d_1 \in D$ such that $d_1|a$ and $d_1|b$. This implies that $d_1\cdot k_1 = a$ and $d_1\cdot k_2 = b$ for $k_1, k_2 \in D$ which implies $a \in (d_1)$ and $b \in (d_1)$. This implies $(a)\subset(d_1)$ and $(b)\subset(d_1)$ which implies $(a,b)\subset(d_1)$. Therefore $(d)\subset(d_1)$ which implies $d \in (d_1)$ or $d = k_3\cdot d_1$ and $d_1|d$. Hence D is a $\mathcal{G.C.D.}$ domain.

Let P be a proper prime ideal of D and let $x \in K$. Then $x = \frac{\alpha}{\beta}$ where $\alpha, \beta \in D$ and $\beta \neq 0$. Now $(\alpha,\beta) = (d)$ for some

$d \in D$ since D is a Bezout domain. This implies that $\alpha = k_1 d$ and $\beta = k_2 \cdot d$ for some $k_1, k_2 \in D$ which implies $\frac{\alpha}{\beta} = \frac{k_1}{k_2}$ and $\frac{\beta}{\alpha} = \frac{k_2}{k_1}$. Suppose $k_1 \in P$ and $k_2 \in P$, then $(k_1) \subset P$ and $(k_2) \subset P$ which implies $(k_1, k_2) \subset P$. But now the greatest common divisor of k_1 and k_2 is 1 from Theorem 2.1. Hence $(k_1, k_2) = (1)$ which implies $(1) \subset P$ and therefore $P = (1)$. This is a contradiction since P is a proper prime ideal of D. Therefore either $k_1 \notin P$ or $k_2 \notin P$ which implies $\frac{k_2}{k_1} \in D_p$ or $\frac{k_1}{k_2} \in D_p$. Hence either $\frac{\alpha}{\beta} \in D_p$ or $\frac{\beta}{\alpha} \in D_p$ which implies $x \in D_p$ or $x^{-1} \in D_p$ and D_p is a valuation ring.

Suppose conversely that D is a $\mathcal{G.C.D.}$ domain and that D_p is a valuation ring for every proper prime ideal P of D. Let $a, b \in D$, then the greatest common divisor of a and b is $d \in D$. We show that $(a,b) = (d)$. Since $d|a$ and $d|b$ then $d \cdot k_1 = a$ and $d \cdot k_2 = b$ for some $k_1, k_2 \in D$ which implies that $(a) \subset (d)$ and $(b) \subset (d)$. Therefore $(a,b) \subset (d)$. Consider $[(a,b):(d)]$ as an ideal of D. If $[(a,b):(d)] = D$, then $(d) \subset (a,b)$ and the theorem is proved. Suppose to the contrary that $[(a,b):(d)] \neq D$, then $[(a,b):(d)] \subset M$ where M is a maximal ideal of D. This implies that $[(a,b):(d)]\, D_M \subset MD_M < D_M$ which implies $[(a,b)D_M : (d)D_m] \subset MD_M < D_M$. Now $\frac{a}{b} = \frac{k_1}{k_2}$ and $\frac{b}{a} = \frac{k_2}{k_1}$ and since D_M is a valuation ring then $\frac{k_1}{k_2} \in D_M$ or

$\frac{k_2}{k_1} \in D_M$ which implies that $\frac{k_1}{k_2} = \frac{r_1}{s_2}$ where $r_1, s_1 \in D$, $s_1 \notin M$ or $\frac{k_2}{k_1} = \frac{r_1}{s_2}$ where $r_2, s_2 \in$, $s_2 \notin M$. This implies that $k_1 \cdot s_1 = k_2 \cdot r_1$ or $k_2 \cdot s_2 = k_1 \cdot r_2$ which implies $k_2 | k_1 \cdot s_1$ or $k_1 | k_2 \cdot s_2$. But now $(k_1, k_2) = 1$ from Theorem 2.1, which implies $k_2 | s_1$ or $k_1 | s_2$ from Theorem 2.3. But if $k_2 | s_1$ then $k_2 \notin M$ and if $k_1 | s_2$ then $k_1 \notin M$, for suppose $k_2 | s_1$ and $k_2 \in M$, then $k_2 \cdot d_1 = s_1$ for some $d_1 \in D$ which implies $s_1 \in M$ which is a contradiction. The same argument holds for k_1. Hence if $\frac{a}{b} = \frac{k_1}{k_2} \in D_M$, then $k_2 \notin M$ and if $\frac{b}{a} = \frac{k_2}{k_1} \in D_M$ then $k_1 \notin M$. Suppose $\frac{a}{b} = \frac{k_1}{k_2} \in D_M$, then $\frac{1}{k_2} \in D_M$ since $k_2 \notin D_M$ which implies that $d = a \cdot 0 + b \cdot \frac{1}{k_2}$. This implies that $d \in (a,b)D_M$ which implies that $(d)D_M \subset (a,b)D_M$ and therefore $1 \in [(a,b)D_M : (d)D_M]$ which is a contradiction since $[(a,b)D_M : (d)D_M] \subset MD_M$. On the other hand suppose $\frac{b}{a} = \frac{k_2}{k_1} \in D_M$, then $\frac{1}{k_1} \in D_M$ since $k_1 \notin M$. This implies that $d = a \cdot \frac{1}{k_1} + b \cdot 0$ which implies that $d \in (a,b)D_M$. Therefore $(d)D_M \subset (a,b)D_M$ and $1 \in [(a,b)D_M : (d)D_M]$ which is a contradiction since $[(a,b)D_M : (d)D_M] \subset MD_M$. But then $[(a,b) : (d)] = D$ and $(d) \subset (a,b)$. Hence $(d) = a,b)$. An obvious induction argument extends to any finitely generated ideal, and therefore D is a Bezout domain.

Definition 2.2: A non-zero element p is prime iff p is not a unit and if $p|ab$ then $p|a$ or $p|b$.

Definition 2.3: A non-zero element q is irreducible iff q is not a unit, and if $q = bc$, then b is a unit or c is a unit.

Theorem 2.13: If D is a *G.C.D.* domain, then $p \in D$ is a prime element iff p is irreducible.

Proof: Suppose p is a prime element of D and that $p = a \cdot b$ where $a,b \in D$. Then since $p = a \cdot b$, $p|a \cdot b$ which implies that $p|a$ or $p|b$. But then $p \cdot k_1 = a$ or $p \cdot k_2 = b$ for some $k_1, k_2 \in D$. This implies that $p = p \cdot k_1 \cdot b$ or $p = p \cdot k_2 \cdot a$ which implies that $1 = k_1 \cdot b$ or $1 = k_2 \cdot a$. Therefore either a or b is a unit.

Suppose conversely that p is an irreducible element of D and that $p|a \cdot b$. Let $(p,a) = d$ where $d \in D$. This implies that $p = k_1 \cdot d$ and $a = k_2 \cdot d$ where $k_1, k_2 \in D$. Since p is irreducible, then d is a unit or k_1 is a unit. If d is a unit, then $d|1$ which implies $(p,a) = 1$ and since D is a *G.C.D.* domain and $p|a \cdot b$ where $(p,a) = 1$, then $p|b$. If k_1 is a unit, then there exists $k_1^{-1} \in D$. Since $d \cdot k_1 = p$ then $d \cdot k_1 \cdot k_1^{-1} = p \cdot k_1^{-1}$ which implies $d = k_1^{-1} \cdot p$. But then $p|d$ and $d|a$ which implies $p|a$. Hence p is a prime element of D.

Theorem 2.14: If D is a *G.C.D.* domain and P is a proper prime ideal of D, then D_p is a *G.C.D.* domain.

Proof: Let D be a proper prime ideal of D. Let $\frac{r_1}{s_1}$, $\frac{r_2}{s_2} \in D_p$. If either $r_1 \notin P$ or $r_2 \notin P$, then $(\frac{r_1}{s_1},\frac{r_2}{s_2}) = 1$. Since if $r_1 \notin P$ or $r_2 \notin P$, then $\frac{s_1}{r_1} \in D_p$ or $\frac{s_2}{r_2} \in D_p$ which implies that either $\frac{r_1}{s_1}$ is a unit or $\frac{r_2}{s_2}$ is a unit and any divisor of a unit is itself a unit and therefore divides 1. Suppose now that $\frac{r_1}{s_1},\frac{r_2}{s_2} \in PD_p$. Then define $(\frac{r_1}{s_1},\frac{r_2}{s_2}) = d$ where $d = (r_1,r_2)$ in D. Since $d = (r_1,r_2)$, then $d \cdot k_1 = r_1$ and $d \cdot k_2 = r_2$ where $(k_1,k_2) = 1$. This implies that $\frac{r_1}{s_1} = d \cdot \frac{k_1}{s_1}$ and $\frac{r_2}{s_2} = d \cdot \frac{k_2}{s_2}$ which implies that $d \mid \frac{r_1}{s_1}$ and $d \mid \frac{r_2}{s_2}$. Suppose $\frac{r}{s} \mid \frac{r_1}{s_1}$ and $\frac{r}{s} \mid \frac{r_2}{s_2}$, then $\frac{r_1}{s_1} = \frac{r}{s} \cdot \frac{\ell_1}{t_1}$ and $\frac{r_2}{s_2} = \frac{r}{s} \cdot \frac{\ell_2}{t_2}$. This implies that $r_1 s t_1 = r s_1 \ell_1$ and that $r_2 s t_2 = r s_2 \ell_2$. Since $s, t_1, t_2 \notin P$ then $s \cdot t_1 \notin P$ and $s \cdot t_2 \notin P$ which implies that $s \cdot t_1 \notin PD_p$ and $s\ t_2 \notin PD_p$. Therefore the $(s \cdot t_2, r) = 1$ and and $(s \cdot t_1, r) = 1$ which implies $r \mid r_1$ and $r \mid r_2$ since $r \mid r_1(st_1)$ and $r \mid r_2(st_2)$. Hence $r \mid d$ which implies $r \cdot k = d$ and therefore $\frac{r}{s} \cdot s \cdot k = d$. Then $d = (\frac{r_1}{s_1},\frac{r_2}{s_2})$ and D_p is a $\mathcal{G}.\mathcal{C}.\mathcal{D}.$ domain.

Theorem 2.15: An integral domain D is quasi-local iff the set N of all non-units of D form the maximal ideal.

Proof: Suppose D is quasi-local, and let N be the set of all non-units of D. Since D is quasi-local there exists a unique maximal ideal M of D. We show M = N. $M \subset N$ is clear. Let $x \in N$, then $(x) \neq D$ which implies $(x) \subset M$ since M is the only maximal ideal of D. This implies $x \in M$ and $N = M$.

Suppose conversely that N forms a maximal ideal of D. Suppose also that there exists a maximal ideal M of D. We show M = N. Now $M \subset N$ is clear which implies that N = D or M = N. $N \neq D$ since $1 \notin N$ which implies M = N. Hence D is quasi-local.

Theorem 2.16: An integral domain D is a valuation ring iff D is a Bezout domain and D is quasi-local.

Proof: Suppose D is a valuation ring. Let $A = (a_1, \ldots, a_n)$ be a finitely generated ideal of D. We use induction on n. If n = 1, then clearly A is principal. Suppose that if A is generated by k generators then A is principal. Suppose $n = k + 1$, then

$$A = (a_1, \ldots, a_k, a_{k+1}) = (a_1, \ldots, a_k) + (a_{k+1}).$$

Now $(a_1, \ldots, a_k) = (d)$ where $d \in D$ which implies that $A = (d, a_{k+1})$ but now since D is a valuation ring either $(d) \subset (a_{k+1})$ or $(a_{k+1}) \subset (d)$. If $(d) \subset (a_{k+1})$, then $A = (a_{k+1})$. If $(a_{k+1}) \subset (d)$ then $A = (d)$. In either case A is principal. Therefore the induction is complete and D is a Bezout domain.

Suppose there exists maximal ideals M_1 and M_2 of D. Since D is a valuation ring then either $M_1 \subset M_2$ or $M_2 \subset M_1$. Suppose $M_1 \subset M_2$. Then this implies that either $M_2 = D$ or

$M_1 = M_2$. Since M_2 is a maximal ideal of D, $M_2 \neq D$. Hence $M_1 = M_2$. Suppose that $M_2 \subset M_1$. Then this implies that either $M_1 = D$ or $M_1 = M_2$. Since M_1 is a maximal ideal of D, then $M_1 \neq D$. Hence $M_1 = M_2$. In either case $M_1 = M_2$ and there is a unique maximal ideal of D. Hence D is quasi-local.

Suppose conversely that D is a Bezout domain, and D is quasi-local. From Theorem 2.12 D_p is a valuation ring for every proper prime ideal P of D. From Theorem 2.15 we know that the set of all non-units N of D form the maximal ideal of D. We show $D = D_N$. $D \subset D_N$ is clear. Let $w \in D_N$, then $w = \frac{r}{s}$, where $r,s \in D$, $s \notin N$. Since $s \notin N$, then $s^{-1} \in D$ which implies that $w = \frac{r}{s} = r \cdot s^{-1} \in D$. Hence $D = D_N$ and therefore D is a valuation ring.

<u>Definition 2.4</u>: A fractional ideal N of D is <u>invertible</u> iff there exists a fractional ideal M such that $N \cdot M = D$. If N is a fractional ideal then $N^{-1} = \{x \in K \mid x N \subset D\}$.

<u>Theorem 2.17</u>: If a fractional ideal N is invertible, then N has a unique inverse M and M = D:N.

<u>Proof</u>: Since N is invertible then there exists a fractional ideal M such that $N \cdot M = D$. We show $M = N^{-1}$. Let $x \in M$. Then $x \cdot N \subset M \cdot N \subset D$ which implies $x \cdot N \subset D$ and $x \in N^{-1}$. Let $x \in N^{-1}$. Then $x \in K$ such that $x \cdot N \subset D$ which implies $x \cdot N \subset M \cdot N$. This implies $x \cdot N \cdot N^{-1} \subset M \cdot N \cdot N^{-1}$ which implies $x \in M$. Hence $M = N^{-1}$. It is clearly unique since if $N \cdot M_1 = D$ then $M_1 = N^{-1} = M$ which implies $M_1 = M$. Also $N^{-1} = D:N$ by definition and so $M = D:N$.

Theorem 2.18: Let A and B be ideals of D. Then A = B iff $AD_p = BD_p$ for every maximal ideal P of D.

Proof: Suppose A = B, then $A^e = B^e$ for any extension of A or B. This implies $AD_p = BD_p$ for every maximal ideal P of D.

Suppose conversely that $AD_p = BD_p$ for every maximal ideal P of D. This implies $\cap AD_p = \cap BD_p$ where the intersection is taken over all maximal ideals P of D. Clearly $A \subset \cap AD_p$. Let $x \in \cap AD_p$. Let $C = \{r \in D | rx \in A\}$. C is an ideal of D. If C = D, then we are through. So suppose $C \neq D$, then $C \subset M$ where M is a maximal ideal of D. But now $x \in AD_M$ which implies $x = \frac{a}{s}$ where $a \in A$ and $s \notin M$. This implies sx = a which implies $s \in C$ which is a contradiction to $C \subset M$. Hence C = D which implies $x \in A$. Therefore $\cap AD_p = A$ and by a similar argument $\cap BD_p = B$ and hence A = B.

Corollary 2.1: If D is an integral domain, then $D = \cap D_p$ where the intersection is over all maximal ideals P of D.

Proof: From the proof of Theorem 2.3, given an ideal A of D, $A = \cap AD_p$ where the intersection is taken over all maximal ideals P of D. But D = (1) and therefore $D = (1) = \cap (1) \cdot D_p = \cap D_p$ where the intersection is taken over all maximal ideals P of D.

Theorem 2.19: (a) If a fractional ideal A of D is invertible, then A is finitely generated.

(b) If A and B are fractional ideals of D such that $A \subset B$ and B is invertible, then there exists a fractional ideal C of D such that $A = B \cdot C$.

(c) A fractional ideal A of D is invertible iff there exists a fractional ideal B of D such that $A \cdot B$ is principal.

Proof: (a) Since A is invertible, then there exists a fractional ideal B of D such that $A \cdot B = D = (1)$. Now this implies that $1 = \sum_{i=1}^{n} a_i \cdot b_i$ where $a_i \in A$ and $b_i \in B$. We show that $A = (a_1, \ldots, a_n)$ $(a_1, \ldots, a_n) \subset A$ is clear since each $a_i \in A$. Let $x \in A$, then $x\ b \in D$ for every $b \in B$. Now

$$x = x \cdot 1 = x \sum_{i=1}^{n} a_i \cdot b_i = \sum_{i=1}^{n} a_i (x \cdot b_i),$$

but $x \cdot b_i \in D$ for every $i \in \{1, 2, \ldots, n\}$. This implies that $(x \cdot b_i)\ a_i \in (a_i)$ for every $i \in \{1, 2, \ldots, n\}$ which implies that $x \in (a_1, \ldots, a_n)$ and $A = (a_1, \ldots, a_n)$.

(b) Since B is invertible, there exists a fractional ideal N such that $B \cdot N = D$. We show $B \cdot (N \cdot A) = A$. Now

$$B \cdot (N \cdot A) = (B \cdot N) \cdot A = D \cdot A \subset A.$$

Let $x \in A$, then $1 \cdot x \in D \cdot A$ which implies $1 \cdot x \in (B \cdot N) \cdot A$. This implies $x \in B \cdot (N \cdot A)$ which implies $B \cdot (NA) \supset A$ and therefore $A = B(N \cdot A)$.

(c) Suppose A is invertible, then there exists a fractional ideal B such that $A \cdot B = D = (1)$ which implies that $A \cdot B$ is principal.

Suppose conversely that $A \cdot B = (x)$ where $x \in K$. Since $x \in K$, then $x = \frac{\alpha}{\beta}$ where $\alpha, \beta \in D$ and $\beta \neq 0$. Now $(\frac{\alpha}{\beta})$ is invertible which implies $A \cdot B(\frac{\beta}{\alpha}) = (\frac{\alpha}{\beta})(\frac{\beta}{\alpha})$ and $A \cdot B(\frac{\beta}{\alpha}) = (1) = D$. Hence A is invertible.

Definition 2.5: D is a Prüfer domain if and only if every non-zero finitely generated ideal is invertible.

Theorem 2.20: The following are equivalent.

(a). D is a Prüfer domain.

(b). Every non-zero ideal of D generated by two elements is invertible.

(c). If $AB = AC$, where A,B, and C are ideals of D, and A is non-zero finitely generated, then $B = C$.

(d). For every proper prime ideal P of D, D_p is a valuation ring.

(e). $A(B \cap C) = AB \cap AC$ for all ideals A, B, C of D.

(f). $(A+B)(A \cap B) = AB$ for all ideals A, B of D.

Proof: (a.) implies (b.) is clear. (b.) implies (a.). Let $C = (c_1, c_2, \ldots, c_n)$ be a non-zero finitely generated ideal of D; we show C is invertible by induction on n. The theorem is true for $n = 1$ and $n = 2$. Suppose $n > 2$ and every non-zero ideal of D generated by $n - 1$ elements is invertible. We may assume that $c_1, c_2, \ldots, c_n$ are all non-zero. Let $A = (c_1, c_2, \ldots, c_{n-1})$, $B = (c_2, c_3, \ldots, c_n)$, $E = (c_1, c_n)$, and $F = c_1 A^{-1} E^{-1} + c_n B^{-1} E^{-1}$. Then we see that

$$CF = [A+(c_n)]c_1A^{-1}E^{-1} + [(c_1)+B]c_nB^{-1}E^{-1}$$
$$= c_1E^{-1} + c_nc_1A^{-1} + c_1c_nB^{-1}E^{-1} + c_nE^{-1}$$
$$= c_1E^{-1}[D+c_nB^{-1}] + c_nE^{-1}[D+c_1A^{-1}]$$

but $c_nB^{-1}\subset D$ and $c_1A^{-1}\subset D$. This implies

$$CF = c_1E^{-1} + c_nE^{-1} = (c_1,c_n)E^{-1} = D.$$

Therefore C is invertible.

(b.) implies (c.).

We know that (b.) implies (a.) from above so we show (a.) implies (c.). Let A, B and C be ideals of D such that $AB = AC$ and A is finitely generated. Then $A^{-1}(AB) = A^{-1}(AC)$ which implies $B = C$. Hence (b.) implies (c.).

(c.) implies (d.).

If A, B and C are ideals of D with $A \neq (0)$ finitely generated and if $AB\subset AC$ then $B\subset C$, for we have $AC = AB + AC = A(B+C)$ which implies $C = B + C$ and therefore $B\subset C$.

Let P be a proper prime ideal of D. We must show that if $\frac{a}{s}$, $\frac{b}{t} \in D_P$, then $(\frac{a}{s})\subset(\frac{b}{t})$ or $(\frac{b}{t})\subset(\frac{a}{s})$. However, since we may assume $s,t \notin P$, then $\frac{1}{s}$ and $\frac{1}{t}$ are units in D_P. Therefore it is sufficient to show that $aD_P\subset bD_P$ or $bD_P\subset aD_P$. This is clear if either $a = 0$ or $b = 0$, so we may assume $a \neq 0$ or $b \neq 0$. It is clear that $(ab)(a,b)\subset(a^2,b^2)(a,b)$ which implies that $(ab)\subset(a^2,b^2)$. This implies that $ab = xa^2 + yb^2$ for some $x,y \in D$ which implies that $(yb)(a,b)\subset(a)(a,b)$ and so $(yb)\subset(a)$. Let $yb = au$ for some $u \in D$. Then $ab = xa^2 + uab$ which implies $xa^2 = ab(1-u)$. If $u \notin P$, then $a = b(\frac{y}{u}) \in bD_P$.

If $u \in P$, then $1 - u \notin P$ and $b = a(\frac{x}{1-u}) \in aD_p$. Hence either $aD_p \subset bD_p$ or $bD_p \subset aD_p$. Therefore D_p is a valuation ring by Theorem 2.11.

(d). implies (e).

Let P be a maximal ideal of D. Then

$$A(B \cap C)D_p = (AD_p)(B \cap C)D_p$$

from Theorem 1.4, but $(AD_p)(B \cap C)D_p = AD_p(BD_p \cap CD_p)$ from Theorem 1.4. Now

$$\begin{aligned} AD_p(BD_p \cap CD_p) &= (AD_pBD_p) \cap (AD_pCD_p) \\ &= ABD_p \cap ACD_p = (AB \cap AC)D_p \end{aligned}$$

since D_p is a valuation ring. Therefore from Theorem 2.18, $A(B \cap C) = AB \cap AC$.

(e.) implies (f.)

Suppose $A(B \cap C) = AB \cap AC$ for all ideals A, B, and C of D. Then

$$\begin{aligned} (A+B)(A \cap B) &= [(A+B)A] \cap [(A+B)B] \\ &= [A^2+AB] \cap [AB+B^2] \supset AB \end{aligned}$$

which implies that $AB \subset (A+B)(A \cap B)$. Now

$$(A+B)(A \cap B) = A(A \cap B) + B(A \cap B)$$

is always true, which implies $(A+B)(A \cap B) = (A^2 \cap AB) + (B^2 \cap AB)$ but now $A^2 \cap AB \subset AB$ and $B^2 \cap AB \subset AB$ which implies that

$$(A^2 \cap AB) + (B^2 \cap AB) \subset AB + AB = AB.$$

Hence

$$(A+B)(A \cap B) \subset AB$$

and therefore

$$(A+B)(A \cap B) = AB.$$

(f.) implies (a.)

We show (f.) implies (b.) and then clearly (f.) implies (a.) since (b.) implies (a.) has already been shown.

Let $C = (c_1, c_2)$ be a non-zero ideal of D generated by two elements. If $c_1 = 0$ or $c_2 = 0$, then clearly C is invertible. Suppose $c_1 \neq 0$ and $c_2 \neq 0$. Then let $A = (c_1)$ and $B = (c_2)$ so that

$$\begin{aligned} C(A \cap B)B^{-1}A^{-1} &= (A+B)(A \cap B)B^{-1}A^{-1} \\ &= AB\,B^{-1}A^{-1} = D. \end{aligned}$$

Thus C is invertible.

<u>Definition 2.6</u>: An overring T of D is <u>flat</u> iff for every prime ideal P of D, either PT = T or $T \subset D_P$.

<u>Theorem 2.21</u>: An overring T of D is flat iff $[(y):(x)] \cdot T = T$ for every $\frac{x}{y} \in T$.

<u>Proof</u>: Suppose T is a flat overring of D, and let $\frac{x}{y} \in T$. Suppose, to the contrary, that $[(y):(x)] \cdot T \neq T$. Then $[(y):(x)] \cdot T \subset M$ where M is a maximal ideal of T. This implies that $M \cap D$ is a prime ideal of D containing $[(y):(x)]$. Since T is a flat overring of D, we know that either $(M \cap D) \cdot T = T$ or $T \subset D_{M \cap D}$. $(M \cap D) \cdot T = T$ is untenable since $(M \cap D)T \subset M$ from Theorem 1.4. This implies that $T \subset D_{M \cap D}$ but now $\frac{x}{y} \in T$ implies $\frac{x}{y} \in D_{M \cap D}$ which implies $\frac{x}{y} = \frac{r}{s}$ where $r, s \in D$ and $s \notin M \cap D$. This implies that sx = ry which implies $s \in [(y):(x)]$. But $[(y):(x)] \subset M \cap D$ which implies $s \in M \cap D$ which is a contradiction to the fact that T is flat.

Suppose conversely that P is a prime ideal of D and that $P \cdot T \neq T$. We show $T \subset D_p$. Let $t \in T$, then $t = \frac{x}{y}$ where $x, y \in D$. Suppose $[(y):(x)]\, D_p \subset P \cdot D_p$. This implies $[(y):(x)] \cdot D_p \cap D \subset P$ which implies $[(y):(x)] \subset P$. This implies that $[(y):(x)] \cdot T \subset P \cdot T$ which implies that $T \subset P \cdot T$. This implies $T = P \cdot T$ which is a contradiction since $P \cdot T \neq T$. Suppose $[(y):(x)] D_p \not\subset P \cdot D_p$. This implies that $[(y):(x)]\, D_p = D_p$ which implies that $1 \in [(y):(x)] \cdot D_p$. This implies that

$1 = \sum_{i=1}^{n} d_i \cdot \frac{r_i}{s_i}$ where $d_i, r_i, s_i \in D$, $s_i \notin P$ and $d_i \in [(y):(x)]$

which implies $d_i(x) \subset (y)$. This implies that $\frac{x}{y} = \sum_{i=1}^{n} \frac{d_i x}{y} \cdot \frac{r_i}{s_i}$

but now $d_i x \in (y)$ which implies that $d_i x = k_i y$ for each i and for some $k_i \in D$. This implies

$$\frac{x}{y} = \sum_{i=1}^{n} \frac{k_i y}{y} \cdot \frac{r_i}{s_i}$$

which implies that

$$\frac{x}{y} = \sum_{n=1}^{n} k_i \cdot \frac{r_i}{s_i} .$$

Therefore $\frac{x}{y} \in D_p$ and $T \subset D_p$. Hence T is a flat overring of D.

<u>Theorem 2.22</u>: The following are equivalent.

(a.) T is a flat overring of D.

(b.) $T_P = D_{P \cap D}$ for every maximal ideal P of T.

(c.) $T = \cap D_{P \cap D}$, where the intersection is taken over all maximal ideals P of T.

<u>Proof</u>: Suppose T is a flat overring of D and let P be a maximal ideal of T. Let $x \in D_{P \cap D}$, then $x = \frac{r}{s}$, where

$r,s \in D$ and $s \notin P\cap D$. This implies $r,s \in T$ and $s \notin P$ which implies $\frac{r}{s} \in T_P$ or $x \in T_P$. Therefore $D_{P\cap D} \subset T_P$. Let $\frac{r}{s} \in T_P$ where $r,s \in T$ and $s \notin P$. This implies $r = \frac{x_1}{y_1}$ and $s = \frac{x_2}{y_2}$ where $x_1, y_1, x_2, y_2 \in D$. Now we can write $r = \frac{x_1 y_1}{y_1 y_2}$ and $s = \frac{x_2 y_1}{y_1 y_2}$. Let $x_1 y_2 = \alpha$, $y_1 y_2 = \beta$, and $x_2 y_1 = \gamma$. Let

$$W = [(\beta):(\alpha)] \cap [(\beta):(\gamma)].$$

We show $W \cdot T = T$. Suppose $W \cdot T \neq T$, then $W \cdot T \subset M$ where M is a maximal ideal of T. Now $M \cap D$ is a prime ideal of D which implies $(M\cap D) \cdot T = T$ or $T \subset D_{M\cap D}$. $(M\cap D)\cdot T = T$ is untenable since $(M\cap D)\cdot T \subset M$ from Theorem 1.4. Therefore $T \subset D_{M\cap D}$. This implies $\frac{\alpha}{\beta}, \frac{\gamma}{\beta} \in D_{M\cap D}$ which implies that $\frac{\alpha}{\beta} = \frac{r_1}{s_1}$ and $\frac{\gamma}{\beta} = \frac{r_2}{s_2}$, where $r_1, r_2, s_1, s_2 \in D$ and $s_1, s_2 \notin M\cap D$. This implies that $s_1 \alpha = r_1 \beta$ and $s_2 \gamma = r_2 \beta$ which implies that $s_1 \cdot s_2 \alpha = s_2 r_1 \beta$ and $s_1 \cdot s_2 \gamma = s_1 r_2 \beta$. This implies that $s_1 \cdot s_2 \in W$ which implies $s_1 \cdot s_2 \in M\cap D$ which is a contradiction since $s_1 \cdot s_2 \notin M\cap D$. Hence $T \not\subset D_{M\cap D}$ but then T is not flat which is a contradiction since T is flat. Hence $W \cdot T = T$.

Now we show $W \cdot D_{P\cap D} = D_{P\cap D}$. Suppose $W \cdot D_{P\cap D} \neq D_{P\cap D}$, then $W \cdot D_{P\cap D}$ is contained in $(P\cap D) \cdot D_{P\cap D}$. This implies $W \subset P\cap D$ which implies $W \cdot T \subset (P\cap D) \cdot T \subset P$ which is a contradiction since $W \cdot T = T$. Hence

$$W \cdot D_{P\cap D} = D_{P\cap D}.$$

This implies that $1 \in W \cdot D_{P \cap D}$ which implies that

$$1 = \sum_{i=1}^{n} d_i \cdot \frac{r_i}{s_i},$$

where $d_i, r_i, s_i \in D$, $s_i \notin P$ and $d_i \notin W$. This implies that $\frac{\alpha}{\gamma} = \sum_{i=1}^{n} \frac{(d_i\alpha)r_i}{\gamma s_i}$. Now $s_i \notin P$ implies s_i is a unit in D_P. Now $s_i \in D_P$ implies $s_i \in W \cdot D_P$ which implies $s_i \in [(\beta):(\gamma)] \cdot D_P$. This implies that $s_i = \frac{u_i}{s'_i}$ where $u_i \in [(\beta):(\gamma)]$ and $s'_i \in D \backslash P$. This implies $s_i^{-1} = \frac{s'_i}{u'_i}$ but now $s_i^{-1} \in D \backslash P$ also which implies $s_i^{-1} \cdot u_i = s'_i$. This implies $u_i \notin P$. Let $d_i \cdot \alpha = k_i \cdot \beta$ and $u_i \cdot \gamma = b_i \cdot \beta$ where $k_i, b_i \in D$ for each i. Now

$$\sum_{n=1}^{n} \frac{(d_i\alpha)r_i}{\gamma s_i} = \sum_{i=1}^{n} \frac{(k_i \cdot \beta)r_i s'_i}{\gamma u_i}$$

but now remember $s = \frac{\gamma}{\beta} \notin P$ which implies that $u_i \cdot \frac{\gamma}{\beta} = b_i \notin P$ for each i. Hence

$$\sum_{i=1}^{n} \frac{(k_i \cdot \beta) \cdot r_i \cdot s_i}{\gamma \cdot u_i} = \sum_{n=1}^{n} \frac{(k_i \cdot \beta) \cdot r_i \cdot s'_i}{b_i \cdot \beta}$$

$$= \sum_{n=1}^{n} \frac{k_i \cdot r_i s'_i}{b_i}$$

is an element of $D_{P \cap D}$. Therefore $\frac{r}{s} = \frac{\alpha}{\gamma}$ is an element of $D_{P \cap D}$ and $T_P \subset D_{P \cap D}$ which implies $T_P = D_{P \cap D}$.

Suppose $T_P = D_{P \cap D}$ for every maximal ideal P of T. Then from Corollary 2.1 $\bigcap T_P = T$ where the intersection is over all maximal ideals P of T. This implies that

$$\cap D_{P\cap D} = \cap T_P = T$$

where the intersection is taken over all maximal ideals P of T.

Suppose $T = \cap D_{P\cap D}$ where the intersection is over all maximal ideals P of T. Let $\frac{x}{y} \in T$. We show that $[(y):(x)]\cdot T = T$. Since $\frac{x}{y} \in T$, then $\frac{x}{y} \in \cap D_{P\cap D}$. Suppose $[(y):(x)]\cdot T \neq T$, then $[(y):(x)]\cdot T \subset M$ where M is a maximal ideal of T. This implies that $\frac{x}{y} \in D_{M\cap D}$ since $\frac{x}{y} \in \cap D_{P\cap D}$ where the intersection is over all maximal ideals P of T. Therefore $\frac{x}{y} = \frac{r}{s}$ where r, $s \in D$ and $S \notin M$. This implies that $sx = ry$ which implies $s \in [(y):(x)]$ which implies that $s \in M\cap D$ since

$$[(y):(x)] \subset [(y):(x)]\cdot T\cap D \subset M\cap D.$$

This is a contradiction since $s \notin M$. Therefore there is no such maximal ideal M and $[(y):(x)]\cdot T = T$.

<u>Theorem 2.23</u>: An integral domain D is a Prüfer domain iff every overring of D is flat.

<u>Proof</u>: Suppose D is a Prüfer domain. Let T be an overring of D, and let P be a maximal ideal of T. We show $T_P = D_{P\cap D}$. It is clear that $D_{P\cap D} \subset T_P$, but since D is a Prüfer domain $D_{P\cap D}$ is a valuation ring. Then from Theorem 1.7 we know that T_P is a valuation ring and that $T_P = [D_{P\cap D}]_P$. Now $(P\cap D)\cdot D_{P\cap D} \subset P$ is clear. But now $P \subset D_{P\cap D}$ from Theorem

1.7 and $1 \notin P$ which implies $P \subset (P \cap D)D_{P \cap D}$. Therefore $P = (P \cap D)D_{P \cap D}$ which implies that P is the set of all non-units. Hence

$$[D_{P \cap D}]_P = D_{P \cap D}$$

and therefore

$$T_P = D_{P \cap D}.$$

From Theorem 2.22, T is flat.

Suppose conversely that every overring of D is flat. Let P be a prime ideal of D. We show D_P is a valuation ring. Let $x \in K$ and suppose that $x \notin D_P$ and $x^{-1} \notin D_P$. This implies that $D_P < D_P[x]$ and $D_P < D_P[x^{-1}]$. Now it is obvious that PD_P is a proper ideal of D_P which implies that $1 \notin PD_P[x]$ or $1 \notin PD_P[x^{-1}]$ from Theorem 1.9. This implies that $D_P[x] \subset D_P$ or $D_P[x^{-1}] \subset D_P$ since both are flat overrings of D. Hence $x \in D_P$ or $x^{-1} \in D_P$ which implies that D_P is a valuation ring and D is a Prüfer domain.

Corollary 2.2: Every overring of a Prüfer domain is a Prüfer domain.

Proof: Let T be an overring of D and let J be an overring of T, i.e., $D \subset T \subset J \subset K$. Let P be a prime ideal of T. Then $P \cap D$ is a prime ideal of D which implies $(P \cap D) \cdot J = J$ or $J \subset D_{P \cap D}$. This implies that $P \cdot J = J$ since $(P \cap D) \cdot J \subset P \cdot J$ or that $J \subset T_P$ since clearly $D_{P \cap D} \subset T_P$. Hence J is a flat overring of T and from Theorem 2.23 , T is a Prüfer domain.

BIBLIOGRAPHY

Zariski, Oscar and Pierre Samuel, Commutative Algebra, Vol. I, (2 volumes), Princeton, New Jersey: D. Van Nostrand Company, Inc., 1958.