QUESTION (HD 0503): Let a, b be integers such that $b^r \mid a^s$ where r, s are natural numbers such that $r \geq s$. Show that $b \mid a$.

ANSWER. There are at least two ways of answering this simple number theory problem. Below we provide the solutions and show the link of this question to some more general multiplicative ideal theory results. First off we note that for r, s as given above $b^r \mid a^s$ implies $b^s \mid a^s$

Solution 1. Suppose that b does not divide a and consider $x = \frac{a}{b}$. Then $\frac{a}{b}$ is not an integer. We can write $x = \frac{a}{b} = \frac{a_1}{b_1}$ such that $\text{GCD}(a_1, b_1) = 1$. Now $b^s \mid a^s$ in Z means that $\frac{a^s}{b^s} = (\frac{a}{b})^s = x^s = (\frac{a_1}{b_1})^s = \frac{a_1^s}{b_1^s}$ is an integer k. So $k = \frac{a_1^s}{b_1^s}$ or $kb_1^s = a_1^s$....(1)

Claim that b_1 is ± 1. For if not then there is a prime factor p of $b_1$and from (1) it follows that $p \mid a_1^s$. But since p is a prime $p \mid a_1^s$ implies that $p \mid a_1$. A contradiction to the fact that $\text{GCD}(a_1, b_1) = 1$.

Now let's recall a few notions from ring theory. Let D be an integral domain with quotient field K. By a "polynomial over D" we usually mean a polynomial in one indeterminate X of the form:$f(X) = \sum_{i=0}^{i=n} a_i X^i$ where $a_i \in D$. If $a_n \neq 0$ then we say that $\deg(f(X)) = n$ and if $a_n = 1$ we say that $f(X)$ is a monic polynomial over D. So a monic polynomial of degree n is of the form: $g(X) = X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0$. An element $\alpha \in K$ is said to be integral over D if the value of a monic polynomial $g(X)$ at $X = \alpha$ is zero, i.e. $g(\alpha) = 0$. Alternatively we say that $\alpha \in K$ is integral over D if α satisfies a monic polynomial over D. We say that D is integrally closed if each $\alpha \in K$ that is integral over D has to be in D. The simplest example of an integrally closed integral domain is the ring of integers Z whose quotient field is Q the field of rational numbers. Here is the reason. Let $\alpha \in Q$ be integral over Z. Then α satisfies some polynomial equation of the form: $\alpha^n + z_{n-1}\alpha^{n-1} + ... + z_1\alpha + z_0 = 0$ where z_i are integers. Now α being rational you can write $\alpha = \frac{r}{s}$ where r, s are integers with $s \neq 0$ and because r, s are integers not both 0 you can cancel out any common factors and assume that $\alpha = \frac{r}{s}$ where r, s are coprime i.e. have GCD 1. So we have $(\frac{r}{s})^n + z_{n-1}(\frac{r}{s})^{n-1} + ... + z_1(\frac{r}{s}) + z_0 = 0$. Multiplying both sides by s^n we get $r^n + z_{n-1}r^{n-1}s + ... + z_1 r s^{n-1} + z_0 s^n = 0$. From this equation it follows that $s \mid r^n$. Since r, s are coprime this cannot hold unless $s = \pm 1$. The fact that Z is integrally closed can be used to give the second solution.

Solution 2. Note that $b^s \mid a^s$ in Z means that $\frac{a^s}{b^s} = (\frac{a}{b})^s = k$ where k is an integer. But then $\frac{a}{b}$ satisfies the equation $X^s - k = 0$ (which is a monic polynomial over Z) and since Z is integrally closed $\frac{a}{b}$ must be in Z and so b must divide a.

(Note that in Solution 2 we did not need to write $\frac{a}{b}$ in the lowest terms.) The next statement can be proved using the same argument as in Solution 2. But for this we need to know what "x divides y" means in an integral domain D. Just as in integers we say that for $x, y \in D$, x divides y (notation $x \mid y$) if there is a $d \in D$ such that $y = xd$.

Observation 3. Let D be an integrally closed integral domain and let $a, b \in$

$D\backslash\{0\}$ such that for some natural number s we have $b^s \mid a^s$ in D. Then $b \mid a$ in D.

The interesting part of the story is that it does not end here. But to be able to read this story you will need to know about

(a) rings of fractions, and of localization D_P at a prime ideal P,

(b) the fact that an invertible ideal in a local ring is principal,

(c) the fact that if if A is an ideal of an integral domain D then $A = \cap AD_M$ where M ranges over all maximal ideals of D,

(d) the fact that if D is integrally closed then every ring of fractions of D is integrally closed.

(e) the notion of star operations discussed in sections 32 and 34 of Gilmer's [Multiplicative Ideal Theory, Marcel Dekker, 1972]

If you do know these topics then read on.

Proposition 4. Let D be an integrally closed integral domain and let I and J be two invertible ideals of D. Suppose that for some natural number n, $I^n \subseteq J^n$ then $I \subseteq J$.

Proof. For each maximal ideal M we have $I^n D_M = (ID_M)^n \subseteq (JD_M)^n$. Since ID_M and JD_M are principal and D_M is integrally closed, by Observation 3, $ID_M \subseteq JD_M$. But then $I = \cap ID_M \subseteq \cap JD_M = J$.

Corollary 4. If I and J are two nonzero ideals in a Dedekind domain with $I^n \subseteq J^n$ then $I \subseteq J$.

In the same fashion but with some more jargon, from Gilmer's book, thrown in we can prove the following result.

Proposition 5. Let D be integrally closed and let I and J be two t-invertible t-ideals such that $I^n \subseteq J^n$ then $I \subseteq J$.

Proof. Let M be a maximal t-ideal of D. Then $(ID_M)^n = I^n D_M \subseteq J^n D_M = (JD_M)^n$. Since ID_M and JD_M are principal and D_M is integrally closed, by Observation 3, $ID_M \subseteq JD_M$. But then $I = \cap ID_M \subseteq \cap JD_M = J$.

Corollary 6. Let I and J be two divisorial ideals in a Krull domain (and in a normal Noetherian domain). If $I^n \subseteq J^n$ for some natural number n then $I \subseteq J$.

Reason: In a Krull domain every divisorial ideal is a t-invertible t-ideal.

The thread does not end here. Recall that if D is an integrally closed integral domain, D is an intersection of valuation overrings. Call a family $\{V_\alpha\}$ of valuation overrings of D a defining family for D if $D = \cap_\alpha V_\alpha$. Each defining family $\{V_\alpha\}$ induces a star operation ϖ on $F(D)$ defined by $A \mapsto A^\varpi = \cap_\alpha AV_\alpha$. With this preparation we have the following statement.

Proposition 7. Let $F = \{V_\alpha\}$ be a defining family of D inducing a star operation ϖ on $F(D)$ and suppose that I and J are two ideals of D such that there are finitely generated ideals A and B with $I^\varpi = A^\varpi$ and $J^\varpi = B^\varpi$. If for some natural number n we have $I^n \subseteq J^n$ then $I^\varpi \subseteq J^\varpi$.

Proof. For each valuation $V_\alpha \in F$, $(I^\varpi V_\alpha)^n = (IV_\alpha)^n = I^n V_\alpha \subseteq J^n V_\alpha = (JV_\alpha)^n = (J^\varpi V_\alpha)^n$. Since for each α, $I^\varpi V_\alpha = IV_\alpha$, $J^\varpi V_\alpha = JV\alpha$ is principal and since a valuation ring is integrally closed we conclude that, for each α, $IV_\alpha \subseteq JV_\alpha$. But then $I^\varpi = \cap IV_\alpha \subseteq \cap JV_\alpha = I^\varpi$.

Corollary 8. Let F be as in Proposition 7 and suppose that each $V_\alpha \in F$ is a DVR of rank one. Then for every nonzero ideals I, J of D, and for every natural number n, $I^n \subseteq J^n$ implies $I \subseteq J^{\varpi}$.

Noe here is a question for the readers to ponder upon.

Question. Let D be an integral domain such that for every pair of integral ideals I, J with $I^n \subseteq J^n$ we have $I \subseteq J$. What kind of a domain is D?

After reading this material, David Anderson remarked that D is a root closed domain if and only if for $a, b \in D\backslash\{0\}$ $b^n | a^n$ implies that $b|a$. Recall that an integral domain D is called root closed if for x in the quotient field K of D, $x^n \in D$ implies that $x \in D$. This means that for every pair $a.b \in D\backslash\{0\}$ with $(\frac{a}{b})^n \in D$ we have $\frac{a}{b} \in D$. Of course an integrally closed domain is root closed, as is apparent from the description above.