QUESTION: (HD1207) Let R be a Prufer domain and suppose that (a^n, b^n) is a principal ideal? Does it imply (a, b) principal?

ANSWER: Not necessarily. Take a non-PID Dedekind domain R with torsion class group. In it there must be a two generated ideal (a, b) that is not principal but $(a, b)^n$ is principal. Now in a Prufer domain $(a, b)^n = (a^n, b^n)$, for all $a, b \in R$. The above mentioned Dedekind domains abound in algebraic number theory. Take an example such as $Z[\sqrt{-5}]$. The ring $Z[\sqrt{-5}]$ is known to be a non-PID Dedekind domain such that $Cl(Z[\sqrt{-5}]) = Z/2Z$. Now $Cl(Z[\sqrt{-5}]) \neq 0$ implies that there is a non-principal prime ideal $P \subseteq Z[\sqrt{-5}]$. Now it is well known that every nonzero (non-principal) ideal of a Dedekind domain is generated by two elements, see e.g. Theorem 38.5 of [Robert Gilmer, Multiplicative Ideal Theory, Dekker, 1972]. So we can take the nonzero non-principal prime ideal P of $Z[\sqrt{-5}]$ to be $P = (a, b)$. Since $|Cl(Z[\sqrt{-5}])| = 2$ we must have $P^2 = (a, b)^2 = (a^2, b^2)$ principal. Example: Take $a = 2$ and $b = 1 + \sqrt{-5}$ in $Z[\sqrt{-5}]$ and verify that (a, b) is non-principal and $(a^2, b^2) = (2)$ in $Z[\sqrt{-5}]$.

However, and this is an exception important enough to include the answer in my helpdesk answers. Let me write it as the following proposition.

Proposition A. Let R be an integrally closed integral domain and let $a, b \in R\backslash\{0\}$ such that (a^n, b^n) is a principal ideal that is generated by an nth power of some element of R then (a, b) is principal.

Proof. Let $(a^n, b^n) = (c^n)$. Then as $a^n, b^n \in (a^n, b^n) = (c^n)$ we have $c^n \mid a^n, b^n$. So $(\frac{a^n}{c^n}, \frac{b^n}{c^n}) = R$. Since R is integrally closed $x^n \mid y^n$ in R implies that $x \mid y$. Thus $c \mid a, b$. Say $a = rc, b = sc$. Then $(a^n, b^n) = (c^n)$ gives $(r^n, s^n) = (1)$. But this means that $(r, s) = (1)$ which gives $(rc, sc) = (c)$ and so $(a, b) = (c)$.

Corollary B. Let R be an integrally closed integral domain such that $a^{\frac{1}{n}} \in R$ for all $a \in R$ and $n \in N$. Then for all $a, b \in R$ and for all $n \in N$, (a^n, b^n) principal implies (a, b) is principal.

Let us recall that an integral domain R is called an almost Bezout (AB-) domain if for each pair $a, b \in R\backslash\{0\}$ there is a positive integer $n = n(a, b)$ such that (a^n, b^n) is principal. This notion was introduced by Dan Anderson and myself in [J. Algebra 142 (2) (1991) 285-309] where it was shown that an integrally closed AB-domain is a Prufer domain with torsion ideal class group and a Prufer domain with torsion ideal class group is an AB-domain. Thus if R is a Dedekind domain with torsion class group then for all $a, b \in R\backslash\{0\}$, there is $n \in N$ and a $c \in R$ such that $(a^n, b^n) = (c)$. If the class group of a given Dedekind domain R is finite of say cardinality m then it is easy to see that for each pair $a, b \in R\backslash\{0\}$ there is a $c \in R$ such that $(a^m, b^m) = (c)$.

Prime examples of Dedekind domains with finite class groups are the rings of integers of algebraic number fields, i.e., finite extensions of the field of rational numbers Q. Let's go back into recall mode and recall that a complex number α is said to be an algebraic number if α satisfies a monic polynomial $X^n + q_{n-1}X^{n-1} + ... + q_1X + q_0$. An algebraic number is called an algebraic integer if the minimal monic polynomial it satisfies happens to have integer coefficients. So an algebraic integer is an algebraic number that is integral over Z. Now let

$\mathcal{K}$ be an algebraic number field and let $\mathcal{O}_{\mathcal{K}}$ the ring of integers of $\mathcal{K}$. Then it is well known that $Cl(\mathcal{O}_{\mathcal{K}})$ is finite (see e.g. Theorem 4.1, page 106 of Cohn [C]([Algebraic Numbers and Algebraic Functions, Chapman and Hall, 1991]). So, given $a, b \in \mathcal{O}_{\mathcal{K}} \backslash \{0\}$ there is an $n \in N$ and a $c \in \mathcal{O}_{\mathcal{K}}$ such that $(a^n, b^n) = (c)$. Next let A be the set of all algebraic integers. Then $A = \{x$ is a complex number such that x is integral over $Z\}$. That A is a ring is straight forward and so is the fact that if α is an algebraic integer then so is $\alpha^{\frac{1}{n}}$. Now, using the above information, we have a simple proof of the following result.

Corollary C. The ring of all algebraic integers is a Bezout domain.

Proof. Let $a, b \in A$, $\mathcal{K} = Q(a, b)$. Then $\mathcal{K}$ is an algebraic number field and $a, b \in \mathcal{O}_{\mathcal{K}}$. But then there is $n \in N$ and $c \in \mathcal{O}_{\mathcal{K}}$ such that $(a^n, b^n) = (c)$ in $\mathcal{O}_{\mathcal{K}}$. But since $c^{\frac{1}{n}} = d \in A$ we conclude that $(a^n, b^n) = (d^n)$, in a ring of integers $\mathcal{O}_{\mathcal{L}}$ of some algebraic number field $\mathcal{L}$. By Proposition A, (a, b) is principal in $\mathcal{O}_{\mathcal{L}}$ and likewise in A. Since a, b were chosen arbitrarily we conclude that every two generated ideal in A is principal.

Let me also mention that Theorem 102 of Kaplansky's book [Commutative Rings, Allyn and Bacon, 1970] can be given a simpler proof similar to that of Corollary C.

It may be easily seen that Corollary C and Theorem 102 of Kaplansky fall under the following statement.

OBSERVATION D. An integral domain R that is a directed union of Prufer domains with torsion class groups is a Prufer domain with torsion class group. If in addition, $c^{\frac{1}{n}} \in R$ for each $c \in R$, then R is a Bezout domain.

Finally and I must point this out, Proposition A can be stated, and proved, for root closed domains. Here a domain R is said to be root closed if for every $x \in K = qf(R)$, $x^n \in R$ implies that $x \in R$ for any positive integer n. Also if R is not root closed one may have some $a, b, c \in R$ such that for some n we have $(a^n, b^n) = (c^n)$ where $(a, b) \neq (c)$. To see this let's recall an example from my paper [Z] ([Manuscripta Math., 51(1985), 29–62]).

Example E. (see [Z, Example 2.13]) Let K be a field with characteristic $p \neq 0$, let L be a purely inseparable extension of K such that $L^P \subset K$ and let X be an indeterminate over L. Construct $R = K + XL[X] = \{a_0 + \sum_{i=1}^{n} a_i X^i : a_0 \in K$ and $a_i \in L\}$. From the illustration given in [Z] one can see that R is a non-integrally closed AB-domain. Now let $l_1.l_2 \in L \backslash K$ such that $\frac{l_1}{l_2} \notin K$. Then $(l_1X, l_2X)R$ is non-principal but $(l_1^p X^p, l_2^p X^p) = (X^p)$ in $K[X]$ and so in R.

Remark 1. (Added at 5:30 PM, 8/3/2012) Somewhere at the back of my head I felt that the arguments were, sort of, familiar. So, I sent, around 1: 00 PM) a copy to Bill Dubuque. He reminded me of a discussion at sci.math, I joined in a few days later, April 2005. You can see it at

http://mathforum.org/kb/message.jspa?messageID=3725752

I must say the main argument was Bill's, this discussion took place in 2005 and ... I have started forgetting things. (How time takes a toll on you!)

I am thankful to Bill and everyone else who joined in that discussion.

Muhammad Zafrullah