BULL. AUSTRAL. MATH. SOC. 13A15
VOL. 49 (1994) [373–376]

IDEALS GENERATED BY POWERS OF ELEMENTS

D.D. ANDERSON, KENT R. KNOPP AND REBECCA L. LEWIN

For an ideal I in a commutative ring R we consider the ideal $I_n = (\{i^n \mid i \in I\})$. We show that if $n!$ is a unit in R, then $I_n = I^n$. We give an example of a doubly generated ideal I with I_3 not finitely generated.

Let R be a commutative ring with identity and let I be an ideal of R. For a natural number n, I^n is of course the ideal of R generated by all the products $i_1 \cdots i_n$ where each $i_s \in I$. It is natural to wonder what happens if instead of taking products $i_1 \cdots i_n$, we take n-th powers of elements from I. Thus we make the following definition, first given in [1].

DEFINITION 1: Let I be an ideal in the commutative ring R and let n be a natural number. Then $I_n = (\{i^n \mid i \in I\})$ is the ideal generated by n th powers of elements of I.

So $I^n \supseteq I_n$ with equality if $n = 1$. Suppose that we are given a generating set for I, $I = (\{a_\alpha\}_{\alpha \in \Lambda})$. Then there is a natural generating set for I^n, namely, $I^n = \left(\{a_{\alpha_1}^{p_1} \cdots a_{\alpha_k}^{p_k} \mid \alpha_i \in \Lambda,\ p_1 + \cdots + p_k = n\}\right)$. Moreover, we have the following containments:

$$I^n \supseteq \left(\left\{\binom{n}{p_1, \cdots, p_k} a_{\alpha_1}^{p_1} \cdots a_{\alpha_k}^{p_k} \mid \alpha_i \in \Lambda,\ p_1 + \cdots + p_k = n\right\}\right) \supseteq I_n \supseteq (\{a_\alpha^n \mid \alpha \in \Lambda\})$$

where $\binom{n}{p_1, \ldots, p_k} = n!/p_1! \cdots p_k!$ is the usual multinomial coefficient. For $n = 1$ all the containments are equalities. For $n = 2$, only the second containment must be an equality. For example, in $\mathbb{Z}[X, Y]$, we have $(X, Y)^2 = \left(X^2, XY, Y^2\right) \supsetneq \left(X^2, 2XY, Y^2\right) = (X, Y)_2 \supsetneq \left(X^2, Y^2\right)$. For $n \geqslant 3$, none of the containments need be equalities. For example, in $\mathbb{Z}[X, Y]$, we have

$$\begin{gathered}(X, Y)^3 = \left(X^3, X^2Y, XY^2, Y^3\right) \supsetneq \left(X^3, 3X^2Y, 3XY^2, Y^3\right) \supsetneq \\ (X, Y)_3 = \left(X^3, 3X^2Y + 3XY^2, 6XY^2, Y^3\right) \supsetneq \left(X^3, Y^3\right).\end{gathered}$$

Received 9th June, 1993

If I is locally principal, then $I^n = (\{a_\alpha^n \mid \alpha \in \Lambda\})$; so $I^n = I_n$. We shall prove (Theorem 5) that for any ideal I, if $n!$ is a unit in R, then $I_n = I^n$.

The ideal I_n, like the ideal I^n, behaves well with respect to localisations and homomorphic images. If S is a multiplicatively closed subset of R, then it is easily proved that $I_{nS} = (I_S)_n$. Thus in many cases we can reduce to the quasi-local case. If $\varphi : R \to T$ is a ring epimorphism, then $\varphi(I_n) = (\varphi(I))_n$.

Since $I_1 = I^1$, the first case of interest is I_2. Suppose that $I = (\{a_\alpha \mid \alpha \in \Lambda\})$. Then it is easily seen that

$$\begin{aligned} I_2 &= \left(\left\{\binom{2}{p_1, p_2} a_{\alpha_1}^{p_1} a_{\alpha_2}^{p_2} \mid \alpha_i \in \Lambda,\ p_1 + p_2 = 2\right\}\right) \\ &= \left(\{a_\alpha^2 \mid \alpha \in \Lambda\} \cup \{2a_\alpha a_\beta \mid \alpha, \beta \in \Lambda,\ \alpha \neq \beta\}\right). \end{aligned}$$

So $(a,b)_2 = (a^2, 2ab, b^2)$. Thus I finitely generated implies that I_2 is finitely generated. As we shall see (Example 4), for I_3 this no longer need be true. Note that if I is locally principal or 2 is a unit in R, then $I^2 = I_2$. We offer the following partial converse.

Theorem 2. *Let (R, M) be a quasi-local integrally closed ring. Let $a, b \in R$ be nonzerodivisors. Then $(a,b)_2 = (a,b)^2$ if and only if either (1) (a,b) is principal or (2) 2 is a unit.*

Proof: We have already remarked that the implication $(\Leftarrow)$ holds. Conversely, suppose that $(a^2, 2ab, b^2) = (a,b)_2 = (a,b)^2$ and that 2 is not a unit. Then $ab = ra^2 + s(2ab) + tb^2$, so $(1-2s)ab = ra^2 + tb^2$. Since $2 \in M$, $1 - 2s$ is a unit, so $ab = ua^2 + vb^2$ for some $u, v \in R$. Dividing both sides by b^2 yields $u(a/b)^2 - a/b + v = 0$. By the u, u^{-1} Lemma [**2**, Theorem 67], either a/b or b/a is in R. In either case, (a,b) is principal. ∎

For $n = 2$, we found a natural basis for I_2 in terms of a basis for I. In particular, if I is finitely generated, so is I_n for $n = 1, 2$. If $n \geqslant 3$ and I is not locally principal, then no such natural basis for I_n exists. In fact, for $n \geqslant 3$, I finitely generated need not even imply that I_n is finitely generated. We show (Example 4) that the ideal $(X,Y)_3$ in $\mathbb{Z}[X, Y, \{T_i\}_{i \in N}]$ is not finitely generated. But first a lemma. Note that Lemma 3 shows that $(X,Y)_3 \subsetneq (X^3, 3X^2Y, 3XY^2, Y^3)$ in $\mathbb{Z}[X,Y]$.

Lemma 3. *Let X and Y be indeterminates over $\mathbb{Z}$. In $\mathbb{Z}[X,Y]$, $(X,Y)_3 = (X^3, Y^3, 3X^2Y + 3XY^2, 6XY^2)$.*

Proof: It is easily checked that $X^3, Y^3, 3X^2Y + 3XY^2, 6XY^2 \in (X,Y)_3$. So the containment $\supseteq$ holds. Now $(fX + gY)^3 = f^3X^3 + 3f^2gX^2Y + 3fg^2XY^2 + g^3Y^3$, so to prove the reverse containment, it suffices to show that $3f^2gX^2Y + 3fg^2XY^2 \in (X^3, Y^3, 3X^2Y + 3XY^2, 6XY^2)$. And to show this it suffices to prove that $fg(fX + gY) \in A = (X + Y, 2Y, X^2, Y^2)$. Note that $XY = (X+Y)Y - Y^2 \in A$.

https://doi.org/10.1017/S0004972700016488 Published online by Cambridge University Press

Let $f = a_0 + a_1X + a_2Y + \cdots$ and $g = b_0 + b_1X + b_2Y + \cdots$. Thus $fX + gY \equiv a_0X + b_0Y \equiv (b_0 - a_0)Y \pmod{A}$. Hence $fg(fX + gY) \equiv a_0b_0(b_0 - a_0)Y \equiv 0 \pmod{A}$ because $a_0b_0(b_0 - a_0)$ is even. ∎

EXAMPLE 4. Let X, Y, and $\{T_i\}_{i\in N}$ be indeterminates over $\mathbb{Z}$. Then for the ideal (X, Y) of $\mathbb{Z}[X, Y, \{T_i\}_{i\in N}]$, $(X, Y)_3$ is not finitely generated.

Let $I = (X, Y)$ in $\mathbb{Z}[X, Y, \{T_i\}_{i\in N}]$. Suppose that I_3 is finitely generated. Now I is generated by elements of the form $(fX + gY)^3 = f^3X^3 + 3f^2gX^2Y + 3fg^2XY^2 + g^3Y^3$. So I_3 finitely generated gives that $I_3 = \left(X^3, Y^3, f_1^2g_1X^2Y + 3f_1g_1^2XY^2, \cdots, 3f_n^2g_nX^2Y + 3f_ng_n^2XY^2\right)$ where $f_1, \cdots, f_n, g_1, \cdots, g_n \in \mathbb{Z}[X, Y, T_1, \cdots, T_{s-1}]$. So we have

$$(*)\qquad \begin{aligned} 3T_s^2X^2Y + 3T_sXY^2 = H_1X^3 + H_2Y^3 + F_1\left(3f_1^2g_1X^2Y + 3f_1g_1^2XY^2\right) + \cdots \\ + F_n\left(3f_n^2g_nX^2Y + 3f_ng_n^2XY^2\right) \end{aligned}$$

where $H_i, F_i \in \mathbb{Z}[X, Y, \{T_i\}_{i\in \mathbb{Z}}]$. Map all the $T_i \to 0$ except for T_s. Then in $(*)$, $f_i, g_i \in \mathbb{Z}[X, Y]$ while $H_i, F_i \in \mathbb{Z}[X, Y, T_s]$. Replacing T_s by a new indeterminate T says that $3T^2X^2Y + 3TXY^2 \in J\mathbb{Z}[X, Y, T] = J\mathbb{Z}[X, Y][T]$ where $J = (X, Y)_3$ in $\mathbb{Z}[X, Y]$. Thus $3XY^2 \in J$. By Lemma 3, $3XY^2 = f_1X^3 + f_2Y^3 + f_3\left(3X^2Y + 3XY^2\right) + f_4\left(6XY^2\right)$ for some $f_i \in \mathbb{Z}[X, Y]$. By degree consideration, we can assume that each $f_i \in \mathbb{Z}$. Clearly $f_1 = f_2 = 0$. Thus $Y = f_3(X + Y) + f_4(2Y)$. Now clearly $f_3 = 0$. Thus $1 = 2f_4$, a contradiction.

In [1] we showed that if R contains a field of characteristic 0, then $I_n = I^n$ for all n. Examples given in [1] show that it is not enough to assume that n is a unit. We next show that if $n!$ is a unit in R, then $I_n = I^n$. The proof given here, using the inclusion-exclusion principle, is different from the proof of the previously mentioned result.

THEOREM 5. *Suppose that R is a commutative ring and I is an ideal of R. If $n!$ is a unit in R, then $I_n = I^n$.*

PROOF: Let $f(X_1, \cdots, X_n) = \sum_{k=1}^{n} \sum_{i(1)<\cdots<i(k)} (-1)^{n-k}\left(X_{i(1)} + \cdots + X_{i(k)}\right)^n$. It suffices to observe that $f(X_1, \cdots, X_n) = n!\, X_1 \cdots X_n$. For then if $n!$ is a unit in R, for $i_1, \cdots, i_n \in I$, we have $i_1 \cdots i_n = (n!)^{-1} f(i_1, \cdots, i_n) \in I_n$. Hence $I^n = I_n$.

That $f(X_1, \cdots, X_n)$ has the desired form may be seen as follows. Note that $f(X_1, \cdots, X_n)$ is a form of degree n. Now clearly $f(0, X_2, \cdots, X_n) = 0$, so $X_1 \mid f$. By symmetry, each $X_i \mid f$, so $f(X_1, \cdots, X_n) = aX_1 \cdots X_n$. Here

$$a = f(1, 1, \cdots, 1) = \sum_{k=1}^{n} \sum_{i(1)<\cdots<i(k)} (-1)^{n-k}k^n = \sum_{k=1}^{n} (-1)^{n-k}\binom{n}{k}k^n = n!.$$

□

We have already remarked that if $I = (\{a_\alpha \mid \alpha \in \Lambda\})$ is locally principal, then $I^n = I_n = (\{a_\alpha^n \mid \alpha \in \Lambda\})$. We end with a related result.

THEOREM 6. *Let a and b be nonzerodivisors in the commutative ring R. Then $(a,b)_n$ locally principal (for example, invertible) implies that $(a,b)_n = (a^n, b^n)$ and hence is invertible.*

PROOF: It is enough to prove that $(a,b)_n = (a^n, b^n)$ locally. Thus we may suppose that (R, M) is a quasi-local ring, a and b are nonzerodivisors in R, and $(a,b)_n$ is principal, say $(a,b)_n = (ra+sb)^n R$. Now $a^n \in (a,b)_n$, so $a^n = \alpha(ra+sb)^n$ for some $\alpha \in R$. If α is a unit, then $b^n \in (a,b)_n = (ra+sb)^n R = a^n R$, so $(a^n, b^n) = a^n R = (a,b)_n$. So assume $\alpha \in M$. Then $a^n = \alpha(ra+sb)^n = \alpha r^n a^n + n\alpha r^{n-1} a^{n-1} sb + \cdots + n\alpha r a s^{n-1} b^{n-1} + \alpha s^n b^n$. Hence $(1 - \alpha r^n) a^n = n\alpha r^{n-1} a^{n-1} sb + \cdots + \alpha s^n b^n$ where $1 - \alpha r^n$ is a unit. Dividing by $(1 - \alpha r^n) b^n$ shows that $a/b \in \overline{R}$, the integral closure of R. Thus $(a,b)\overline{R} = b\overline{R}$ is principal; so $(a,b)^n \overline{R} = b^n \overline{R} = (a^n, b^n)\overline{R}$. Now $(a^n, b^n) \supseteq (a,b)_n$ where $(a,b)_n$ is principal; so $(a^n, b^n) = A(a,b)_n$ for some ideal A of R. Now $(a,b)^n \overline{R} = (a^n, b^n)\overline{R} = A(a,b)_n \overline{R} = (A\overline{R})((a,b)_n \overline{R}) \subseteq (A\overline{R})(a,b)^n \overline{R}$. Hence $A\overline{R} = \overline{R}$ since $(a,b)^n$ is finitely generated. But since $R \subseteq \overline{R}$ is integral, $A\overline{R} = \overline{R}$ gives that $A = R$. So $(a^n, b^n) = (a,b)_n$. □

REFERENCES

[1] D.D. Anderson and M. Zafrullah, 'Almost Bézout domains', *J. Algebra* **142** (1991), 285–309.

[2] I. Kaplansky, *Commutative Rings*, Revised Edition (University of Chicago Press, Chicago, 1974).

Department of Mathematics
The University of Iowa
Iowa City, IA 52242
United States of America

Department of Mathematics
Mt. Mercy College
Cedar Rapids, IA 52402
United States of America

Department of Mathematics
University of Wisconsin – La Crosse
La Crosse, WI 54601
United States of America