7. Suppose that $I \lhd R$ is finitely generated. Show that $I^2 = I$ if and only if $I = (e)$ for some idempotent element $e \in R$. Give an example of a ring with a nil ideal satisfying $I^2 = I$. *(N. Praterelli, M. Roy)*

Proof. Let $I \lhd R$ be finitely generated.

(i) Suppose that $I = (e)$ where $e \in R$ is an idempotent. Then $I^2 = (e^2) = (e) = I$.

(ii) Suppose that $I^2 = I$.

We shall first consider the case $I = (a)$ for some element $a \in R$. Then $(a) = I = I^2 = (a^2)$, so $ra^2 = a$ for some $r \in R$. Let $e = ra$. Then $e^2 = (ra)^2 = r(ra^2) = ra = e$, so e is an idempotent. Also, $ea = (ra)a = ra^2 = a$, so that $I \subseteq (e)$. But $e = ra$, so $(e) \subseteq I$ and so $I = (e)$.

Next, we consider the case $I = (a, b)$ for some elements $a, b \in R$. Then

$$a, b \in I = I^2 = (a^2, ab, b^2),$$

so that

$$\begin{aligned} a &= u_1a^2 + v_1ab + w_1b^2 = (u_1a + v_1b)a + (w_1b)b \text{ and} \\ b &= u_2a^2 + v_2ab + w_2b^2 = (u_2a + v_2b)a + (w_2b)b \end{aligned}$$

for some $u_1, v_1, w_1, u_2, v_2, w_2 \in R$. Set $p = u_1a + v_1b$, $q = w_1b$, $r = u_2a + v_2b$, and $s = w_2b$. Note that $p, q, r, s \in I$. Then, if we set

$$M = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in M_2(I),$$

we have that $\begin{bmatrix} a \\ b \end{bmatrix} = M \begin{bmatrix} a \\ b \end{bmatrix}$. Set $e = \mathrm{tr}(M) - \det(M) = (p + s) - (ps - qr)$. (We shall discuss the motivation for this choice at the end of this section of the proof.) Now, we have

$$\begin{aligned} qb - sa &= q(ra + sb) - s(pa + qb) = qra + qsb - psa - qsb = qra - psa \text{ and} \\ ra - pb &= r(pa + qb) - p(ra + ps) = pra + qrb - pra - psb = qrb - psb, \end{aligned}$$

so

$$\begin{aligned} ea &= pa + sa - psa + qra = pa + sa + (qb - sa) = pa + qb = a \text{ and} \\ eb &= pb + sb - psb + qrb = pb + sb + (ra - pb) = ra + sb = b. \end{aligned}$$

Then, for all $z = xa + yb \in I$, we have $ze = (xa + yb)e = xa + yb = z$, so that $I = (e)$. Additionally, setting $z = e$, we see that $e^2 = e$.

Finally, we consider the case that I is n-generated where $n > 2$. We shall proceed by induction on n. Suppose that the result holds for $(n-1)$-generated ideals and that $I = (a_1, \ldots, a_n)$. Let $J = (a_1, \ldots, a_{n-1})$ and $K = (a_n)$ so that $I = J + K$. Then, $J/K = (J+K)/K = I/K = (a_1 + K, \ldots, a_{n-1} + K)$ so that J is $(n-1)$-generated and $(J/K)^2 = J/K$. Then, by the induction hypothesis, $J/K = (f + K)$ for some idempotent $f + K \in R/K$ and so J is generated by f and some collection of elements from K (although f is no longer necessarily an idempotent in R). Then, $I = J + K = (f, a_n)$ is 2-generated and so by the $n = 2$ case above, $I = (e)$ for some idempotent $e \in R$.

We shall now briefly discuss the motivation for the choice of e in the $n = 2$ case. By problem #9 of this set, we know that the Cayley-Hamilton Theorem holds for any commutative ring. Thus, if we let

$$p_M(x) = x^2 - \mathrm{tr}(M)x + \det(M)$$

be the minimum polynomial for M, then $p_M(M) = 0$. Note that the coefficients of p_M are in I, so that if there were an element $e \in I$ such that $ze = z$ for all $z \in I$, then we would expect that $p_M(e) = 0$, since M acts as the identity transformation on $\begin{bmatrix} a & b \end{bmatrix}^{\mathrm{T}}$. Formally solving the equation $p_M(e) = 0$ for e, we see that $e = \mathrm{tr}(M) - \det(M)$. While we handled the case $n > 2$ by induction, this method suggests that we could explicitly compute the idempotent e by finding an $n \times n$ matrix $M \in M_n(I)$ which acts as the identity transformation on $\begin{bmatrix} x_1 & \ldots & x_n \end{bmatrix}^{\mathrm{T}}$, setting $p_M(e) = 0$ under the hypothesis that $ze = z$ for all $z \in I$, and solving formally for e.

$\square$