

Let $yz \in I$. Assume for a contradiction that $y \notin I$ and $z \notin I$. By maximality of I , both ideal $I + \langle y \rangle$ and ideal $I + \langle z \rangle$ do not belong to Σ . This implies $x^n \in I + \langle y \rangle$ and $x^m \in I + \langle z \rangle$ for some $n, m > 0$, which cause a contradiction to $I \in \Sigma$, since $x^{n+m} \in I + \langle yz \rangle = I$. ■

Let I be an ideal of the ring R . By the term **radical** of I , we mean $\sqrt{I} \triangleq \{x \in R : x^n \in I \text{ for some } n > 0\}$, which is equivalent to the preimage of $\text{Nil}(R/I)$ under the quotient map and equivalent⁴ to the intersection of all prime ideals of R that contain I .

⁴This follows from the fact that the correspondence between the ideals of R and the ideals of R/I induces a bijection between $\text{Spec}(R)$ and $\text{Spec}(R/I)$.

1.2 Script 1

I proved and gathered the propositions in my paragraphs.

Theorem 1.2.1. (Ideal Quotients are well defined) If we define for each pair I, S of ideals of R their **ideal quotient** by

$$(I : S) \triangleq \{x \in R : xy \in I \text{ for all } y \in S\}$$

Then $(I : S)$ forms an ideal.

Proof. To see $(I : S)$ is closed under addition, let $x, z \in I, y \in S$, and observe

$$(x + z)y = xy + zy \in I$$

To see $(I : S)$ is a multiplicative black hole, let $u \in (I : S), v \in R, s \in S$ and observe

$$(uv)s = v(us) \in I \text{ because } us \in I$$

■

Theorem 1.2.2. (Description of annihilator) Given some ideal I of R , we use the notation $\text{Ann}(I)$ to denote its **annihilator** $(\{0\} : I)$. We have

$$\text{Ann}(I) = \{x \in R : xy = 0 \text{ for all } y \in I\}$$

Proof. Obvious.

■

Given a principal ideal $\langle x \rangle$, we shall always denote its annihilator simply by $\text{Ann}(x)$

Theorem 1.2.3. (Description of the set of zero-divisors) If we denote D the set of zero-divisors of R , we have

$$D = \bigcup_{x \neq 0 \in R} \text{Ann}(x)$$

Proof. If d is a zero-divisor, then $d \in \text{Ann}(s)$ for the $s \neq 0$ that divides 0 with d . If $x \neq 0$ and $y \in \text{Ann}(x)$, then $yx = 0$.

■

Theorem 1.2.4. (An example) Let $R \triangleq \mathbb{Z}, I \triangleq \langle m \rangle$ and $S \triangleq \langle n \rangle$. We have

$$(I : S) = \langle q \rangle$$

Where

$$q = \frac{m}{(m, n)} \text{ and } (m, n) \text{ is the highest common factor of } m \text{ and } n.$$

Proof. To show $\langle q \rangle \subseteq (I : S)$, we only have to show $q \in (I : S)$. Let p be arbitrary integer so pn is an arbitrary element of S . Note that

$$m \mid mp \cdot \frac{n}{(m, n)} = q(pn) \implies q(pn) \in I$$

Because pn is an arbitrary element of S , we have shown $q \in (I : S)$. To show $(I : S) \subseteq \langle q \rangle$, let $p \in (I : S)$. Because $p \in (I : S)$, we know $pn \in I$. That is,

$$m \mid pn$$

Dividing both side with (m, n) , we see

$$q \mid p \cdot \frac{n}{(m, n)}$$

Because $q = \frac{m}{(m, n)}$ is by definition coprime with $\frac{n}{(m, n)}$, we can now deduce

$$q \mid p$$

as desired. ■

Question 1

Let I, S, T, V_α be ideals of ring R . Show

- (a) $I \subseteq (I : S)$.
- (b) $(I : S)S \subseteq I$.
- (c) $((I : S) : T) = (I : ST) = ((I : T) : S)$.
- (d) $(\bigcap V_\alpha : S) = \bigcap (V_\alpha : S)$.
- (e) $(I : \sum V_\alpha) = \bigcap (I : V_\alpha)$.

Proof. Proposition (a) is obvious. Proposition (b) is also obvious once we reduce the problem into proving the single sum xy belongs to I where $x \in (I : S)$ and $y \in S$. For proposition (c), we first show

$$((I : S) : T) \subseteq (I : ST)$$

Because ideal is closed under addition, we only have to prove $xst \in I$ where $x \in ((I : S) : T)$, $s \in S$ and $t \in T$, which follows from noting $xt \in (I : S)$. (done) . Note that

$$(I : ST) \subseteq ((I : T) : S)$$

is obvious. (done) . Lastly, we show

$$((I : T) : S) \subseteq ((I : S) : T)$$

Let $x \in ((I : T) : S)$, $t \in T$ and $s \in S$. We are required to show $xts \in I$, which is obvious since $xs \in (I : T)$. (done) . Proposition (d) is obvious. Let $x \in (I : \sum V_\alpha)$. Fix α and $r \in V_\alpha$. Because $r \in \sum V_\alpha$, we see $xr \in I$. Let x be in the intersection, it is clear that $x \sum v_\alpha = \sum xv_\alpha \in I$ because $xv_\alpha \in I$. ■

Theorem 1.2.5. (Radicals of ideals are well-defined) If I is an ideal of R , then the radical of I defined by

$$r(I) \triangleq \{x \in R : x^n \in I \text{ for some } n > 0\}$$

is also an ideal.

Proof. To see $r(I)$ is closed under addition, let $x^n, y^m \in I$, and observe $(x + y)^{n+m} \in I$. To see $r(I)$ is a multiplicative black hole, let $x^n \in I, v \in R$ and observe $(xv)^n = x^n v^n \in I$. ■

Theorem 1.2.6. (Description of Radicals) Let $\pi : R \rightarrow R/I$ be the quotient map. We have

$$r(I) = \pi^{-1}(\text{Nil}(R/I))$$

Proof. Obvious. ■

Question 2

- (a) $I \subseteq r(I)$.
- (b) $r(r(I)) = r(I)$.
- (c) $r(IS) = r(I \cap S) = r(I) \cap r(S)$
- (d) $r(I) = R \iff I = R$.
- (e) $r(I + S) = r(r(I) + r(S))$.
- (f) If I is prime, then $r(I^n) = I$ for all $n > 0$.

Proof. Proposition (a) and (b) are obvious. The proposition

$$r(IS) \subseteq r(I \cap S)$$

follows from $IS \subseteq I \cap S$. The propositions

$$r(I \cap S) \subseteq r(I) \cap r(S) \text{ and } r(I) \cap r(S) \subseteq r(IS)$$

are clear, thus proving proposition (c). The proposition

$$I = R \implies r(I) = R$$

is clear, and its converse follows from $1 \in r(I) \implies 1 = 1^n \in I$, thus proving proposition (d). The proposition

$$r(I + S) \subseteq r(r(I) + r(S))$$

is clear. Let $x^n = y + z$ where $y^m \in I$ and $z^p \in S$. We see $x^{n(m+p)} \in I + S$. We have shown

$$r(r(I) + r(S)) \subseteq r(I + S)$$

thus proving proposition (e). Let I be prime. We know $I \subseteq r(I)$. To see the converse, let $x^n \in I$. Because I is prime, either x or x^{n-1} belongs to I . If x does not belong to I , then x^{n-1} belongs to I , which implies either $x \in I$ or $x^{n-2} \in I$. Applying the same argument repeatedly, we see $x \in I$, thus proving $r(I) \subseteq I$. Because

$$I \supseteq I^2 \supseteq I^3 \supseteq I^4 \supseteq \dots$$

we know

$$r(I) \supseteq r(I^2) \supseteq r(I^3) \supseteq r(I^4) \supseteq \dots$$

Because

$$x^n \in I \implies x^{nk} \in I^k \text{ for all } k \in \mathbb{N}$$

We now also have

$$r(I) \subseteq r(I^k) \text{ for all } k \in \mathbb{N}$$

This proved proposition (e). ■

Theorem 1.2.7. (Description of radical) Let I be an ideal of R .

$$r(I) = \bigcap \{S \in \text{spec}(R) : I \subseteq S\}$$