

MA557 Problem Set 1

Carlos Salinas

September 12, 2015

Problem 1.1

Show that $\text{rad}(R[X]) = \text{nil}(R[X])$.

Proof. We will first prove the following results (which can be found in Dummit and Foote, §7.3, p. 33):

Lemma 1. *Let $f = a_n X^n + \dots + a_0 \in R[X]$. Then*

- (a) *f is nilpotent in $R[X]$ if and only if a_0, a_1, \dots, a_n are nilpotent elements of R ;*
- (b) *f is a unit in $R[X]$ if and only if a_0 is a unit and a_1, \dots, a_n are nilpotent in R .*

Proof of lemma. (a) \Leftarrow : Suppose that a_0, \dots, a_n are nilpotent. Then $a_0, \dots, a_n \in \text{nil}(R)$, hence $f \in \text{nil}(R) \subset \text{nil}(R[X])$. \Rightarrow : Conversely, if $f^k = 0$ for some positive integer k , then $(a_n X^n)^k = 0$, so $a_n^k X^{nk} \in \text{nil}(R[X])$ so $f - a_n X^n \in \text{nil}(R[X])$, in particular $a_n \in \text{nil}(R[X])$. By induction on n , $a_0, \dots, a_n \in \text{nil}(R[X])$.

(b) \Leftarrow : Suppose a_0 is unit and a_1, \dots, a_n are nilpotent. Then, by (a), $f - a_0 = a_n X^n + \dots + a_1 X$ is nilpotent so $f - a_0 \in \text{rad}(R[X])$. By Proposition 1.13, f is a unit. \Rightarrow : On the other hand, if f is a unit, there exist $g = b_m X^m + \dots + b_0$ in $R[X]$ with $fg = 1$. Now, let \mathfrak{p} be an arbitrary prime ideal. Since f is a unit in $R[X]$, $\bar{f} = \bar{a}_n X^n + \dots + \bar{a}_0$ is a unit in $R[X]/\mathfrak{p}$. But since $R[X]/\mathfrak{p}$ is an integral domain and \bar{f} is a unit, $\deg \bar{f} = 0$ so $\bar{a}_i = 0$ for every $i \in \{1, \dots, n\}$. Since \mathfrak{p} was chosen arbitrarily, \diamond

By definition $\text{rad}(R)$ is the intersection of every maximal (hence prime) ideal of R so, by Theorem 1.12, $\text{rad}(R) \supset \text{nil}(R)$. To see the reverse containment let $f = a_n X^n + \dots + a_0$ be in $\text{rad}(R[X])$. By Proposition 1.13, $1 + fg$ is a unit for every $g \in R[X]$. In particular, $1 + fX$ is a unit, so by Lemma 1(b), a_0, \dots, a_n are nilpotent so $f \in \text{nil}(R[X])$. (Alternatively, one can look at $R[X]$ as a subring of $R[[X]]$ and note that since $1 - f$ is invertible and $(1 - f)^{-1} = \sum f^k$ in the power series ring, $f^n = 0$ for some n since $(1 - f)^{-1} \in R[X]$. That is, f is nilpotent.) \blacksquare

Problem 1.2

Let I and J be R -ideals. Show that

$$\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}.$$

Proof. $\sqrt{IJ} = \sqrt{I \cap J}$: By contradiction, suppose that there exists some prime ideal $\mathfrak{p} \supset IJ$, but $\mathfrak{p} \not\supset I \cap J$. Then there exists some element $x \in I \cap J$ with $x \notin \mathfrak{p}$. However, $x^2 \in IJ$. This contradicts the primality of \mathfrak{p} . Hence, if \mathfrak{p} is a prime ideal containing IJ , it must also contain $I \cap J$ so $\sqrt{IJ} = \sqrt{I \cap J}$.

$\sqrt{IJ} = \sqrt{I} \cap \sqrt{J}$: Let $x \in \sqrt{I} \cap \sqrt{J}$. Then $x^n \in I$ for some $n > 0$ and $x^m \in J$ for some $m > 0$. Then $x^{n+m} \in IJ$ so $x \in \sqrt{IJ}$. Hence $\sqrt{IJ} \supset \sqrt{I} \cap \sqrt{J}$. To see the reverse containment note that, by above, since $\sqrt{IJ} = \sqrt{I \cap J}$, then $x \in \sqrt{IJ}$ implies $x^n \in I$ and $x^n \in J$ for some $n > 0$, hence $x \in \sqrt{I} \cap \sqrt{J}$ so $\sqrt{IJ} = \sqrt{I} \cap \sqrt{J}$.

By transitivity of “=”, it follows that $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$. ■

Problem 1.3

Let S be a subset of a ring R . Show that the following are equivalent:

- (i) $R \setminus S$ is a union of prime ideals.
- (ii) $1 \in S$, and for any elements x, y of R , $x \in S$ and $y \in S$ if and only if $xy \in S$.

Proof. (ii) \implies (i): Suppose that S is a saturated multiplicative subset of R . Then $S \supset R^\times$ so every element of $R \setminus S$ is a non-unit. By Corollary 1.5, for every $x \in R \setminus S$, there exists a maximal ideal $\mathfrak{m} \supset (x)$. Hence

$$R \setminus S = \bigcup_{\mathfrak{m} \supset (x)} \mathfrak{m},$$

in particular $R \setminus S$ is a union of prime ideals.

(i) \implies (ii): Suppose that $R \setminus S$ is a union of prime ideals. Then, it is clear that $R^\times \subset S$ so $1 \in S$. Now $x, y \in S$ if and only if $x, y \notin R \setminus S$ if and only if $xy \notin \mathfrak{p}$ for some prime ideal $\mathfrak{p} \subset R \setminus S$. Hence, S is a saturated multiplicative subset of R , i.e., satisfies the conditions given in (ii). ■

Problem 1.4

Show that the set of all zero divisors in a ring is a union of prime ideals.

Proof. By Problem 1.3, it suffices to show that the complement of the set of all zero-divisors, call it Z , of a ring R is a saturated multiplicative subset. It is clear that $R \setminus Z \supset R^\times$ (since, if $u \in R^\times$, $ub = 0$ if and only if $b = 0$: \implies is easily seen since $u^{-1}ub = 1 \cdot b = 0$ so $b = 0$; the converse is immediate). Now, xy in R is a zero-divisor if and only if x or y are zero-divisors, hence (by taking the negation of this statement) $xy \in R \setminus Z$ implies $x, y \in R \setminus Z$. Thus, $R \setminus Z$ is a saturated multiplicative subset of R . ■

Problem 1.5

Let $\varphi: R \rightarrow S$ be a surjective homomorphism of rings.

- (a) Show that $\varphi(\text{rad}(R)) \subset \text{rad}(S)$, but that equality does not hold in general.
- (b) Show that $\varphi(\text{rad}(R)) = \text{rad}(S)$ if R is semilocal.

Proof. (a) The containment $\varphi(\text{rad}(R)) \subset \text{rad}(S)$ follows easily from Proposition 1.13: $x \in \text{rad}(R)$ if and only if $1 + xy$ is a unit for every $y \in R$. Then

$$\begin{aligned}\varphi(1 + xy) &= \varphi(1) + \varphi(xy) \\ &= \varphi(1) + \varphi(x)\varphi(y) \\ &= 1 + \varphi(x)\varphi(y).\end{aligned}$$

Since φ is surjective, $1 + \varphi(x)s$ is a unit for every $s \in S$ so $\varphi(x) \in \text{rad}(S)$.

To see that equality does not hold in general, take R to be \mathbf{Z} and S to be $\mathbf{Z}/(6)$. Then the canonical projection $\pi: R \rightarrow S$ is a surjection. Since R is a domain, $\text{rad}(R) = 0$, but $\text{rad}(S) = 3S \cap 2S \neq 0 = \varphi(0) = \varphi(\text{rad}(R))$.

(b) By part (a) we have that $\varphi(\text{rad}(R)) \subset \text{rad}(S)$ so we need only show the reverse containment. Now, suppose R is semilocal with maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_n$. Then, by Corollary 1.15, $\text{rad}(R) = \bigcap_{i=1}^n \mathfrak{m}_i$. Now, by the Homeomorphism Theorem, $S \cong R/\ker \varphi$ so, by Proposition 1.2, the maximal ideals of S are in one-one correspondence with the maximal ideals of R that contain $\ker \varphi$. Assuming $S \neq 0$, $\ker \varphi \neq R$ so, by Corollary 1.5, at least one of the maximal ideals $\mathfrak{m}_i \supset \ker \varphi$. Without loss of generality, assume the first k maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_k$ contain $\ker \varphi$ and the last $\mathfrak{m}_{k+1}, \dots, \mathfrak{m}_n$ do not. Since $\ker \varphi \not\subset \mathfrak{m}_i$ for $k+1 \leq i \leq n$, $\ker \varphi + \mathfrak{m}_i = R$, i.e., $\ker \varphi$ and \mathfrak{m}_i are comaximal, so there exists elements $y \in \ker \varphi$ and $x_i \in \mathfrak{m}_i$ such that $y + x_i = 1$. Then

$$\begin{aligned}\varphi(\text{rad}(R)) &= \varphi(\mathfrak{m}_1 \cdots \mathfrak{m}_k \mathfrak{m}_{k+1} \cdots \mathfrak{m}_n) \\ &= \mathfrak{n}_1 \cdots \mathfrak{n}_k \varphi(\mathfrak{m}_{k+1} \cdots \mathfrak{m}_n) \\ &= \mathfrak{n}_1 \cdots \mathfrak{n}_k R \\ &= \mathfrak{n}_1 \cdots \mathfrak{n}_k\end{aligned}$$

■

Problem 1.6

An element $e \in R$ is called *idempotent* if $e^2 = e$. Show that in a local ring, 0 and 1 are the only idempotents.

Proof. Suppose R is a local ring with maximal ideal \mathfrak{m} . Suppose, by contradiction, that there exists some $e \in R$, $e \neq 0$ or 1 , with $e^2 = e$. Then $e^2 - e = e(e - 1) = 0$ so e and $e - 1$ are zero-divisors, in particular, e and $e - 1$ are non-units and hence contained in the maximal ideal \mathfrak{m} . But then $e - (e - 1) = 1 \in \mathfrak{m}$. This contradicts the maximality of \mathfrak{m} . ■

Problem 1.7

Let I be an R -ideal. Show that I is finitely generated and $I^2 = I$ if and only if $I = Re$ with e idempotent.

Proof. The direction \Leftarrow (that is $I = (e)$ with e idempotent) is immediate by the definition of the product of ideals (namely $I^2 \subset I$, but, since $e^2 = e$, $e \in I^2$ so $I^2 \supset I$).

\Rightarrow Conversely, by Nakayama's lemma (Theorem 2.2), if we view I as a finitely generated R -module, then $I = I^2$ if and only if $xI = 0$ for some $x \in 1 + I$. First, note that $1 - x$ is idempotent since

$$(1 - x)(1 - x) = 1 - x.$$

Now, for any element $y \in I$, we have

$$(1 - x)y = y - xy = y.$$

This implies that any element of I is of the form $(1 - x)z$ for $z \in R$. This gives the inclusion $I \subset (1 - x)$. Thus, since $I \supset (1 - x)$, we have that $I = (1 - x)$. ■