Graduate Algebra
Homework 8

Fall 2014

Due 2014-11-12 at the beginning of class

Throughout this problem set R is a commutative ring. Recall that $\mathfrak{p} \subset R$ is a prime ideal if $\mathfrak{p} \neq R$ and $R/\mathfrak{p}$ is an integral domain, and $\mathfrak{m} \subset R$ is a maximal ideal if $\mathfrak{m} \neq R$ and $R/\mathfrak{m}$ is a field.

1. Let R be a commutative ring.

   (a) If $\mathfrak{p}$ is a prime ideal of R show that $\mathfrak{p}[X] \subset R[X]$ is a prime ideal. Is $\mathfrak{m}[X] \subset R[X]$ a maximal ideal for a prime ideal $\mathfrak{m}$ of R?

   (b) Suppose $\sqrt{-5} \in R$. Show that $(2, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (1-\sqrt{-5})$ as ideals.

   (c) Let $I \subset R$ be an ideal. Show that there exists a bijection between the set of all/prime/maximal ideals of R containing I and the set of all/prime/maximal ideals of R/I.

   Proof. (a): $R[X]/\mathfrak{p}[X] \cong (R/\mathfrak{p})[X]$. $\mathfrak{p}$ is prime so $R/\mathfrak{p}$ is a domain so $(R/\mathfrak{p})[X]$ is a domain so $\mathfrak{p}[X]$ is a prime. But $(R/\mathfrak{p})[X]$ is never a field so $\mathfrak{m}[X]$ is not maximal.

   (b): Let $\alpha = \sqrt{-5}$.

   $$\begin{aligned}(2, 1+\alpha)(3, 1-\alpha) &= (6, 2-2\alpha, 3+3\alpha, 6)\\ &= (6, 2-2\alpha, 3+3\alpha)\\ &= (6, 2-2\alpha, 5+\alpha)\\ &= (6, 2-2\alpha, 1-\alpha)\\ &= (1-\alpha)\end{aligned}$$

   where in line 3 added the last two gens of line 2, in line 4 subtracted last gen from the first. Finally $2-2\alpha = 2(1-\alpha)$ and $6 = (1+\alpha)(1-\alpha)$ so we conclude what we wanted.

   (c): Take $\pi : R \to R/I$. Know that if J is an ideal of R/I then $\pi^*(J) = \pi^{-1}(J)$ is an ideal of R which necessarily contains $I = \ker pi$. Moreover, π^* takes prime ideals to prime ideals. Also $R/\pi^*(J) \cong \operatorname{Im}\overline{\pi}$ and
   overlineπ is surjective since π is. Thus $R/\pi^*(J) \cong (R/I)/J$ so if J is maximal then $\pi^*(J)$ is maximal. If J is an ideal of R containing I then $\pi_*(J) = \pi(J)R/I = (J/I)(R/I) = J/I = \pi(J)$ and $R/J \cong (R/I)/(J/I)$ so again $\pi_*(J)$ is prime/maximal iff J is prime/maximal. Finally, $\pi^*\pi_*(J) = \pi^{-1}(J/I) = J + I = J$ and $\pi_*\pi^*(J) = \pi\pi^{-1}(J) = J$ so the maps π^* and π_* are bijections. □

2. Let R be a commutative ring. A **minimal prime ideal** in R is a prime ideal $\mathfrak{p}$ such that if $\mathfrak{q} \subset \mathfrak{p}$ is a prime ideal of R then $\mathfrak{q} = \mathfrak{p}$. Show that every prime ideal $\mathfrak{p}$ contains a nonzero minimal prime ideal. [Hint: Zorn's lemma.]

   Proof. Let S be the set of prime ideals $\mathfrak{q} \subset \mathfrak{p}$. Since $\mathfrak{p} \in S$ the set S is nonempty. Partially order the set S wrt inclusion, i.e., $\mathfrak{q} < \mathfrak{q}'$ if $\mathfrak{q} \supset \mathfrak{q}'$. Suppose T is an ascending chain in S. Let $\mathfrak{q}_T = \cap_{\mathfrak{q}\in T}\mathfrak{q}$. Then $\mathfrak{q}_T$ is an ideal (any intersection of ideals is an ideal). Suppose $xy \in \mathfrak{q}_T$. Then $xy \in \mathfrak{q}$ for any $\mathfrak{q} \in T$ and so one of x or y is in $\mathfrak{q}$. Suppose $y \notin \mathfrak{q}_T$. The $y \notin \mathfrak{q}$ for some $\mathfrak{q} \in T$ and so $y \notin \mathfrak{q}'$ for any $\mathfrak{q}' \in T$ such that $\mathfrak{q} \supset \mathfrak{q}'$. This implies that $x \in \mathfrak{q}'$ and so $x \in \mathfrak{q}_T$. Thus $\mathfrak{q}_T$ is a prime ideal.

We conclude, using Zorn's lemma, that S has a maximal element and so $\mathfrak{p}$ contains a minimal prime ideal. □

3. (a) Let $I, J, \mathfrak{a} \subset R$ be ideals such that $\mathfrak{a} \subset I \cup J$ show that $\mathfrak{a} \subset I$ or $\mathfrak{a} \subset J$.
   (b) Suppose $\mathfrak{p}$ is a prime ideal of R and $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subset R$ are ideals such that $\cap \mathfrak{a}_i \subset \mathfrak{p}$. Show that $\mathfrak{a}_i \subset \mathfrak{p}$ for some i.

Proof. (a): Suppose $\mathfrak{a}$ is not in I or J. Then pick $x \in \mathfrak{a} - I$ and $y \in \mathfrak{a} - J$ in which case, since $\mathfrak{a} \subset I \cup J$ we deduce that $x \in J$ and $y \in I$. Now $x + y \in \mathfrak{a} \subset I \cup J$. If $x + y \in I$ we deduce that $x \in I$ as well, a contradiction. Similarly for $x + y \in J$.

(b): Suppose we can find $x_i \in \mathfrak{a}_i - \mathfrak{p}$. Then $\prod x_i \in \cap \mathfrak{a}_i \subset \mathfrak{p}$ and so $\prod x_i \in \mathfrak{p}$. But this cannot be since $\mathfrak{p}$ is a prime ideal and we'd get that one of the x_i is in $\mathfrak{p}$. □

4. Let $\mathfrak{a}, \mathfrak{b} \subset R$ be ideals. Define the **ideal quotient** $(\mathfrak{a} : \mathfrak{b}) = \{x \in R | x\mathfrak{b} \subset \mathfrak{a}\}$.
   (a) Show that $(\mathfrak{a} : \mathfrak{b})$ is an ideal of R.
   (b) Show that $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subset \mathfrak{a} \subset (\mathfrak{a} : \mathfrak{b})$ and that if $\mathfrak{c}$ is another ideal then $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c})$.
   (c) If $m, n \in \mathbb{Z} - 0$ compute $((m) : (n))$ as an ideal of $\mathbb{Z}$.
   (d) Compute $((2, X) : (3, X))$, $((6, X) : (2, X))$ and $((6) : (3, X))$ in $\mathbb{Z}[X]$.

Proof. (a): Pick $x, y \in (\mathfrak{a} : \mathfrak{b})$ and $r \in R$. Then $x\mathfrak{b} \subset \mathfrak{a}$ and $y\mathfrak{b} \subset \mathfrak{a}$. But $(x + ry)\mathfrak{b} = x\mathfrak{b} + ry\mathfrak{b} \subset \mathfrak{a} + r\mathfrak{a} = \mathfrak{a}$ and so $x + yr \in (\mathfrak{a} : \mathfrak{b})$ so the quotient is an ideal.

(b): If $x \in \mathfrak{a}$ then $x\mathfrak{b} \subset \mathfrak{a}$ immediately as $\mathfrak{a}$ is an ideal. That $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subset \mathfrak{a}$ follows from the definition. Now suppose $x \in R$ such that $x\mathfrak{c} \subset (\mathfrak{a} : \mathfrak{b})$. Thus $x\mathfrak{c}\mathfrak{b} \subset \mathfrak{a}$ which implies $x \in (\mathfrak{a} : \mathfrak{b}\mathfrak{c})$. The converse is identical.

(c): See $a \in \mathbb{Z}$ such that $(a)(n) \subset (m)$, i.e., $m \mid na$. Dividing by (m, n) this is equivalent to $m/(m, n) \mid n/(m, n)a$ and since $m/(m, n)$ and $n/(m, n)$ are coprime it must be that $m/(m, n) \mid a$. Thus $((m) : (n)) = (m/(m, n))$.

(d): You can do this explicitly but here is a better way. If $I \subset R$ and $\mathfrak{a}, \mathfrak{b}$ contain I then I claim that $(\mathfrak{a} : \mathfrak{b})$ is the preimage of $(\mathfrak{a}/I : \mathfrak{b}/I)$ under the projection $R \to R/I$. Indeed, if $x\mathfrak{b} \subset \mathfrak{a}$ then immediately $x\mathfrak{b}/I \subset \mathfrak{a}/I$. If $(x + I)\mathfrak{b}/I \subset \mathfrak{a}/I$ it follows that $x\mathfrak{b} \subset \mathfrak{a} + I = \mathfrak{a}$.

First we apply the observation to $I = (X)$. Thus $((2, X) : (3, X))$ is the preimage in $\mathbb{Z}[X]$ of $((2) : (3))$ in $\mathbb{Z} = \mathbb{Z}[X]/(X)$. But this is (2) from the previous part. Thus $((2, X) : (3, X)) = (2, X)$. Similarly $((6, X) : (2, X)) = \pi^{-1}(((6) : (2))) = \pi^{-1}((3)) = (3, X)$.

$$\begin{aligned} ((6) : (3, X)) &= \{P(X) | P(X)(3, X) \subset (6)\} \\ &= \{P(X) | P(3Q + XR) \subset 6\mathbb{Z}[X], \forall Q, R\} \end{aligned}$$

In particular this should be true for $Q = 0, R = 1$ so $6 \mid PX$ which implies $6 \mid P$. Thus $((6) : (3, X)) \subset (6) \subset ((6) : (3, X))$ so $((6) : (3, X)) = (6)$. □

5. (a) Show that $P(X) = a_0 + a_1 X + a_2 X^2 + \cdots \in R[\![X]\!]$ is invertible if and only if $a_0 \in R^\times$.
   (b) Show that in any commutative ring the sum of a unit and a nilpotent is a unit.
   (c) Show that $P(X) = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$ is invertible if and only if $a_0 \in R^\times$ and $a_1, \dots, a_n$ are nilpotent. [Hint: If $g(X) = b_0 + b_1 X + \cdots + b_m X^m$ is its inverse show that $a_n^{r+1} b_{m-r} = 0$ for all $0 \le r \le m$ by induction. Then use the previous part.]

(d) Show that $P(X)$ is nilpotent if and only if $a_0, \dots, a_n$ are all nilpotent.

(e) Show that in $R[X]$ the nilradical is the same as the Jacobson radical.

(f) Compute $\sqrt{(xy, y^3)}$ in $\mathbb{C}[x, y]$ and $\sqrt{(108)}$ in $\mathbb{Z}$.

Proof. (a): If $Q(X) = b_0 + b_1 X + \cdots$ then

$$P(X)Q(X) = \sum_{i,j} a_i b_j X^{i+j} = \sum_n X^n \sum_{i+j=n} a_i b_j$$

Thus $PQ = 1$ yields iff

$$\begin{aligned} a_0 b_0 &= 1 \\ a_1 b_0 + a_0 b_1 &= 0 \\ &\vdots \end{aligned}$$

If P is invertible the first condition implies $a_0 \in R^\times$. Now suppose $a_0 \in R^\times$. Then we can iteratively compute

$$b_n = -a_0^{-1}(a_n b_0 + \cdots + a_1 b_{n-1})$$

and so we can produce Q as an inverse of P.

(b): Suppose $x \in R^\times$ and $u^n = 0$. Then

$$\begin{aligned} \frac{1}{x+u} &= \frac{u^{-1}}{1 + xu^{-1}} \\ &= u^{-1} \sum_{k \geq 0} (xu^{-1})^k \\ &= u^{-1}(1 + (xu^{-1}) + (xu^{-1})^2 + \cdots + (xu^{-1})^{n-1}) \end{aligned}$$

since $u^n = 0$ the inverse is truncated.

(c): Have

$$P(X)Q(X) = a_n b_m X^{m+n} + (a_n b_{m-1} + a_{n-1} b_m) X^{m+n-1} + \cdots$$

The base case is $r = 0$ and immediately $a_n b_m = 0$ as $PQ = 1$. Suppose $a_n^r b_{m-r+1} = 0$ for some $0 \leq r \leq m$. We'd like to deduce it for r. Look at the coefficient of X^{m+n-r} of degree $\geq n$. The coefficient vanishes and so

$$a_n b_{m-r} + a_{n-1} b_{m-r+1} + \cdots = 0$$

and multiplying with a_n^r we get

$$a_n^{r+1} b_{m-r} + \sum a_{n-i} a_n^r b_{m-(r-i)} = 0$$

The inductive hypothesis implies that only the first term survives and so $a_n^{r+1} b_{m-r} = 0$.

For $r = m$ we deduce that $a_n^{m+1} = 0$ so a_n is nilpotent.

We now show the statement by induction on $\deg P$. If $P(X)$ is invertible then we know that a_n and so also $a_n X^n$ is nilpotent so by the previous part $P(X) - a_n X^n$ is invertible of degree $n - 1$. By the inductive hypothesis we deduce that a_0 is invertible and $a_1, \dots, a_{n-1}$ are nilpotent.

Now suppose a_0 is invertible and a_i is nilpotent for $i \geq 1$. Then $a_i X^i$ are nilpotent so $a_1 X + \cdots + a_n X^n$ is nilpotent. Again the previous part then implies that adding the unit a_0 gives P is invertible.

(d): If a_i are nilpotent then $a_i X^i$ are and so their sum P is nilpotent. If P is nilpotent then $XP(X)$ is nilpotent so $1 + XP(X)$ is a unit and we can use the previous part.

(e): We know that $\mathrm{Nil}(R[X]) \subset J(R[X])$ so we need that if $P(X)$ is in the Jacobson radical then it is nilpotent. But then for all polynomials Q, $1 - PQ$ is a unit. For $Q = X$ we deduce that a_i are all nilpotent so P is nilpotent as desired.

(d): Seek polynomials $P(x,y)$ such that $P(x,y)^n \in (xy, y^3)$ for some n. Then $y \mid P^n$ and so $y \mid P$. If $P = yQ$ then $P^3 = y^3Q^3 \in (xy, y^3)$ so $\sqrt{(xy, y^3)} = (y)$.

Seek $n \in \mathbb{Z}$ such that n^k is divisible by $108 = 2^2 \cdot 3^3$. But then n is divisible by 2 and 3 and so by 6. If $n = 6m$ then $n^3 = 216m^3$ is divisible by 108. So $\sqrt{(108)} = (6)$. $\square$