Math 510b: Homework 1

Peter Kagey

January 23, 2019

Problem 5.3.

(i) Given an example of a commutative ring containing two prime ideals P and Q for which $P \cap Q$ is not a prime ideal.

(ii) If $P_1 \supseteq P_2 \supseteq \ldots \supseteq P_n \supseteq \ldots$ is a decreasing sequence of prime ideals in a commutative ring R, prove that $\bigcap_{n \geq 1} P_n$ is a prime ideal.

Proof.

(i) Let $R = \mathbb{Z}$ and let $P = (2)$ and $Q = (3)$. Then $P \cap Q = (6)$, which is not a prime ideal because $2 \cdot 3 \in (6)$, but $2, 3 \notin (6)$.

(ii) Let $P = \bigcap_{n \geq 1} P_n$, and note that for all $n \in \mathbb{N}, P \subseteq P_n$. This implies that P is a proper ideal, because $P \subseteq P_1 \subsetneq R$. Next let $ab \in P$. Since $P \subseteq P_n$ for all n, this means that for all $n \in \mathbb{N}$, $ab \in P_n$ and $a \in P_n$ or $b \in P_n$. Thus since $a \in P_n$ for all n or $b \in P_n$ for all n, either a or b is in the intersection P.

□

Problem 5.6. Prove that the ideal $I = \left(x^2 - 2, y^2 + 1, z\right) \subseteq \mathbb{Q}[x, y, z]$ is a proper ideal.

Proof. It is sufficient to show that $1 \notin I = \{(x^2 - 2)q_1 + (y^2 + 1)q_2 + zq_3 : q_1, q_2, q_3 \in \mathbb{Q}\}$. If $f(x, y, z) = (x^2 - 2)q_1 + (y^2 + 1)q_2 + zq_3$ with q_1, q_2, or q_3 not equal to zero, then $\deg(f) \geq 1$ because $\mathbb{Q}$ is a field of characteristic zero. If $q_1 = q_2 = q_3 = 0$, then $f(x, y, z) = 0$. Thus there are no elements in $f(x) \in I$ with $\deg(f) = \deg(1) = 0$, and so I is a proper ideal. □

Problem 5.13. A commutative ring R is a local ring if it has a unique maximal ideal.

(i) If p is a prime, prove that the ring of p-adic fractions

$$\mathbb{Z}_p = \{a/b \in \mathbb{Q} : p \nmid b\},$$

is a local ring.

(ii) If k is a field, prove that the ring $k[[x]]$ of all power series is a local ring.

(iii) If R is a local ring with unique maximal ideal $\mathfrak{m}$ prove that $a \in R$ is a unit if and only if $a \notin \mathfrak{m}$.

Proof.

(i) Let $M = (p)$. Then $\mathbb{Z}_p/\,(p)$ is a field, and so M is maximal:
Let $\overline{a/b} \neq \overline{0}$ be the equivalence class of a/b in $\mathbb{Z}_p/\,(p)$. Then $p \nmid a$ and $p \nmid b$. Thus $(\overline{a/b})^{-1} = \overline{b/a}$, so $\mathbb{Z}_p/\,(p)$ is a field.

This M is unique because

(ii) Let $M = (x)$. Then $k[[x]]/\,(x)$ with quotient map which sends

$$\sum_{n=0}^{\infty} a_n x^n \mapsto a_0.$$

is clearly isomorphic to k, a field.

(iii) By the hint, assume that every non-unit in a commutative ring lies in some maximal ideal.
($\Longrightarrow$) Assume that $a \in R$ is a unit.
($\Longleftarrow$). Assume that $a \notin \mathfrak{m}$.

$\square$

Problem 5.17. Prove that a UFD R is a PID if and only if every nonzero prime ideal is a maximal ideal.

Proof.
($\Longrightarrow$) Assume that R is a PID, let $\langle p \rangle \subset R$ be a nonzero prime ideal, and let $\langle m \rangle$ be another ideal such that $\langle p \rangle \subseteq \langle m \rangle \subsetneq R$. Thus $m \mid p$, but since p is prime. Note that m is not a unit, since $\langle m \rangle \neq R$, so since p is prime (and thus irreducible), $p = um$ with u a unit, so $\langle p \rangle = \langle m \rangle$, and thus $\langle p \rangle$ is maximal.

($\Longleftarrow$). Let $\mathcal{S} = \{J \triangleleft R : I \subseteq J \text{ is not principal}\}$. It is enough to show that $\mathcal{S}$ is empty.
Assume that $\{S_n\}$ is a chain of proper ideals in $\mathcal{S}$ such that $S_i \subseteq S_{i+1}$. Now the union $S = \bigcup_n S_n$ cannot be principal because if $S = (r)$, then there exists some i such that $r \in S_i$ and thus $S_i = (r)$. A contradiction because S_i is not principal due to its inclusion in $\mathcal{S}$.

Therefore S is maximal and non-principal, so by Zorn's Lemma, $\mathcal{S}$ has a maximal element, M. Note that M is not a prime ideal of R because all prime ideals are principal. Thus there exists some $ab \in M$ such that $a, b \notin M$, so $M \subsetneq M + (a) \subsetneq R$ and $M \subsetneq M + (b) \subsetneq R$, so these must be principal ideals. However, if they are, then $M = (M+(a))(M+(b)) = (a)(b) = (ab)$, a contradiction to the claim that M is not principal.

Thus $\mathcal{S}$ is empty, so all ideals are principal, meaning R is a PID. $\square$

Problem 5.23. Prove that $f(x,y) = xy^3 + x^2y^2 - x^5y + x^2 + 1$ is an irreducible polynomial in $\mathbb{R}[x,y]$.

Proof. Consider f as a polynomial in y over $\mathbb{R}[x]$. Then x^2+1 is irreducible in $\mathbb{R}[x]$

$$\begin{aligned} f(x,y) &= xy^3 + x^2y^2 - x^5y + (x^2+1) \\ &= y(xy^2 + x^2y - x^5) + (x^2+1) \end{aligned}$$

$\square$

Problem 5.24. Let
$$D = \det\left(\begin{bmatrix} x & y \\ z & w \end{bmatrix}\right) = xw - yz \in \mathbb{Z}[x, y, z, w].$$

1. Prove that (D) is a prime ideal in $\mathbb{Z}[x, y, z, w]$.
2. Prove that $\mathbb{Z}[x, y, z, w]/(D)$ is not a UFD.

Proof.

1. Since $\mathbb{Z}[x, y, z, w]$ is a UFD (by induction with base case $\mathbb{Z}$) it is enough to show that D is an irreducible element. Since z is prime view D as a polynomial in w over $[x, y, z]$. Then $z \mid -yz$, $z^2 \nmid -yz$, and $z \nmid xw$, so by Eisenstein's criteria, D is irreducible. Therefore D is prime, and thus (D) is a prime ideal.
2. Notice that in this ring $\bar{x}\bar{w} = \bar{y}\bar{z}$, and $\bar{x}, \bar{y}, \bar{z}, \bar{w}$ are prime, and are all distinct up to unit.

$\square$

Problem 5.40. Prove that every non-unit in a commutative ring lies in some maximal ideal.

Proof. On the first day of class we saw the corollary of Zorn's lemma which states

> If $1 \in R$ and $I \neq R$ is any proper ideal of R (left, right, or two-sided), then there exists a maximal ideal M such that $I \subseteq M \subset R$.

We know that if $a \in R$ is a non-unit, then $\langle a \rangle$ is a proper ideal of R, and in particular, $1 \notin \langle a \rangle$ and thus $\langle a \rangle$ fulfills the hypotheses of the corollary. $\square$

Problem 8. Let R be the ring of integers in $F = \mathbb{Q}[\sqrt{m}]$. Show that

1. if $m \cong 2, 3 \bmod 4$ then $R = \mathbb{Z}[\sqrt{m}]$, and
2. if $m \cong 1 \bmod 4$ then $R = \mathbb{Z}[a]$, where $a = (1 + \sqrt{m})/2$.

Proof.

1. The elements of $\mathbb{Q}[\sqrt{m}]$ look like $a + b\sqrt{m}$ with $a, b \in \mathbb{Q}$, and so have monic (and hence minimal) polynomial
$$(x - a)^2 - b^2 m = x^2 - 2ax + (a^2 - b^2 m)$$
which by construction this has $a + b\sqrt{m}$ as a root. In order for $\alpha = a + b\sqrt{m}$ to be in R, $-2a$ and $a^2 - b^2 m$ must be integers. (So surely $\mathbb{Z}[\sqrt{m}] \in R$) Thus $a = c/2$.

   If c is even (i.e. $a \in \mathbb{Z}$), then it is sufficient that $b^2 m$ is an integer—but this occurs precisely when the denominator of b divides m at least twice. Thus if c is even, $\alpha = a + b\sqrt{m}$ with $a, b \in \mathbb{Z}$.

   If c is odd, that is, it can be written as $c = 2k + 1$, then
$$a^2 - b^2 m = \frac{(2k+1)^2 - 4b^2 m}{4} = \frac{4k^2 + 4k + 1 - 4b^2 m}{4}$$
which is not an integer if $b \in \mathbb{Z}$, because the numerator is not divisible by 4. (In particular, it is congruent to 1 mod 4.) Thus $b/2 = d$ where d is odd. In other words, $2b = 2j + 1$, and
$$a^2 - b^2 m = \frac{4k^2 + 4k + 1 - (2j+1)^2 m}{4} = \frac{4k^2 + 4k + 1 - (4j^2 + 4j + 1)m}{4}.$$
So this case only occurs when $m \equiv 1 \bmod 4$, therefore $R = \mathbb{Z}[\sqrt{m}]$ for $m \not\equiv 1 \bmod 4$.

2. When $m \equiv 1 \bmod 4$, R has elements of the form $a + b\sqrt{m}$ and $k + \frac{1}{2} + (j + \frac{1}{2})\sqrt{m}$, which have minimal polynomials $x^2 - 2ax + a^2 - b^2 m$ and
$$x^2 - (2k+1)x + \left(k + \frac{1}{2}\right)^2 - \left(j + \frac{1}{2}\right)^2 m$$
which has roots
$$\frac{(2k+1) \pm (2j+1)\sqrt{m}}{2} = \frac{(2k+1) \pm (2j+1)\sqrt{m}}{2}$$
and thus $F = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$.

$\square$