Homework 3

9.1.4. Claim: The ideal (x) of $\mathbb{Q}[x,y]$ is prime but not maximal. The ideal (x,y) in $\mathbb{Q}[x,y]$ is maximal.

Proof: Consider first the map

$$\phi\colon \mathbb{Q}[x,y] \to \mathbb{Q}[y]$$

where

$$\phi(f(x,y)) := f(0,y).$$

First, I claim ϕ is well-defined. If

$$f(x,y) = \sum_{j=0}^{n}\sum_{i=0}^{j} a_{i,j}x^i y^{j-i}$$

is an element of $\mathbb{Q}[x,y]$, then

$$\phi(f(x,y)) = \sum_{j=0}^{n}\sum_{i=0}^{j} a_{i,j}0^i y^{j-i} = \sum_{j=0,n} a_{0,j}y^j \in \mathbb{Q}[y].$$

Now I claim ϕ is a ring homomorphism. Suppose $f(x,y) = \sum_{j=0}^{n}\sum_{i=0}^{j} a_{i,j}x^i y^{j-i}$ and $g(x,y) = \sum_{j=0}^{m}\sum_{i=0}^{j} b_{i,j}x^i y^{j-i}$ are in $\mathbb{Q}[x,y]$, and say $n \geq m$. For convenience, define $b_{i,j} = 0$ for $i + j > m$. Then

$$\phi(f(x,y) + g(x,y)) = \sum_{j=0}^{n}(a_{0,j} + b_{0,j})y^j = \phi(f(x,y)) + \phi(g(x,y)).$$

Also,

$$\phi(f(x,y)g(x,y)) = \sum_{j=0}^{n}\sum_{k=0}^{j}(a_{0,k}b_{0,j-k})y^j = \phi(f(x,y))\phi(g(x,y)).$$

This shows ϕ is a ring homomorphism.

The kernel of ϕ is the set of polynomials which ϕ sends to 0. These are polynomials all of whose terms contain an x. That is, the kernel of ϕ is exactly (x). Hence by the First Isomorphism Theorem for rings, $\mathbb{Q}[x,y]/(x) \cong \mathbb{Q}[y]$. We know that $\mathbb{Q}[y]$ is an integral domain. Hence (x) is prime. Since $\mathbb{Q}[y]$ is not a field, (x) is not maximal.

Now consider the map

$$\rho\colon \mathbb{Q}[x,y] \to \mathbb{Q}$$

defined by

$$\rho(f(x,y)) := f(0,0).$$

First, I claim this map is well-defined. If

$$f(x,y) = \sum_{j=0}^{n} \sum_{i=0}^{j} a_{i,j} x^i y^{j-i},$$

then

$$\rho(f(x,y)) = a_{0,0}$$

is an element of $\mathbb{Q}$.

Now I claim this map is a ring homomorphism. Suppose $f(x,y) = \sum_{j=0}^{n} \sum_{i=0}^{j} a_{i,j} x^i y^{j-i}$ and $g(x,y) = \sum_{j=0}^{m} \sum_{i=0}^{j} b_{i,j} x^i y^{j-i}$ are in $\mathbb{Q}[x,y]$, and say $n \geq m$. Again for convenience, define $b_{i,j} = 0$ for $i + j > m$. Then

$$\rho(f(x,y) + g(x,y)) = a_{0,0} + b_{0,0} = \phi(f(x,y)) + \phi(g(x,y)).$$

Also,

$$\rho(f(x,y)g(x,y)) = a_{0,0}b_{0,0} = \phi(f(x,y))\phi(g(x,y)).$$

This shows ϕ is a ring homomorphism.

The kernel of this ring homomorphism is the set of polynomials with no constant term. This is exactly the ideal (x,y). Hence, by the First Isomorphism Theorem, $\mathbb{Q}[x,y]/(x,y) \cong \mathbb{Q}$. Since $\mathbb{Q}$ is a field, (x,y) is a maximal ideal.

9.2.1. Claim: If F is a field, and $f(x) \in F[x]$ is a polynomial of degree n, then for every $\overline{g(x)} \in F[x]/(f(x))$, there is a unique polynomial $g_0(x)$ of degree $\leq n-1$ such that $\overline{g(x)} = \overline{g_0(x)}$.

Proof: Suppose $g(x) \in F[x]$ is nonzero. Then by Theorem 9.3, there exist unique polynomials $q(x)$ and $r(x)$ in $F[x]$ so that

$$g(x) = q(x)f(x) + r(x),$$

and either $r(x) = 0$ or the degree of $r(x)$ is less than n. Set $g_0(x) = r(x)$. Then since $g(x) - g_0(x) = q(x)f(x) \in (f(x))$, $\overline{g(x)} = \overline{g_0(x)} \in F[x]/(f(x))$.

Now suppose there were another $g_0'(x)$ whose degree were smaller than n, and such that $\overline{g(x)} = \overline{g_0'(x)} \in F[x]/(f(x))$. Then there would exist $q'(x)$ such that $g(x) = q'(x)f(x) + g_0'(x)$. This would contradict the uniqueness of this decomposition in Theorem 9.3, hence $g_0'(x) = g_0(x)$ is unique.

9.2.5. Claim: Suppose F is a field, and $p(x) \in F[x]$. Then all ideals of $F[x]/(p(x))$ are of the form

Proof: First, by the Fourth Isomorphism Theorem for rings, $I/(p(x))$ is an ideal of $F[x]/(p(x))$ if and only if I is an ideal of $F[x]$ containing $p(x)$. By Theorem 9.3 $F[x]$ is a Euclidean Domain, and hence a Principal Ideal Domain. Hence all ideals of $F[x]$ are of the form $I = (f(x))$ for some $f(x) \in F[x]$. Then $(f(x)) \supseteq (p(x))$ if and only if $f(x)$ divides $p(x)$.

Since $F[x]$ is a Unique Factorization Domain, we can write $p(x) = p_1(x)p_2(x)\cdots p_n(x)$ for some irreducible polynomials $p_i(x)$ which are unique up to associates. Since associate elements of a ring generate the same ideal (Proposition 8.3), we then know that the ideals of $F[x]$ containing $p(x)$ are exactly the ideals of the form $(p_{i_1}(x)\cdots p_{i_s}(x))$ for some subset $\{i_1,\ldots,i_s\}$ of $\{1,\ldots,n\}$. We can then conclude that the ideals of $F[x]/(p(x))$ are all of the form $(p_{i_1}(x)\cdots p_{i_s}(x))/(p(x))$.

9.3.4. Let $R = \mathbb{Z} + x\mathbb{Q}[x]$.

(a) Claim: R is an integral domain, whose units are ± 1.

Proof: The ring R is a subring of $\mathbb{Q}[x]$, which is an integral domain. Hence R is an integral domain. Further, suppose $f(x)g(x) = 1$. Since we have a degree norm on R which is additive, the degree of $f(x)$ and $g(x)$ must be 0. Then $f(x)$ and $g(x)$ must be constants which are units in $\mathbb{Z}$. Hence the units in R are ± 1.

(b) Claim: The irreducibles in R are $\pm p$ where p is prime in $\mathbb{Z}$, and polynomials $f(x)$ which are irreducible in $\mathbb{Q}[x]$ and have constant term ± 1. These irreducibles are prime in R.

Proof: Suppose first $f(x)$ is of the form $\pm p$ for some prime $p \in \mathbb{Z}$. If $f(x)$ could be a written as a product $f(x) = a(x)b(x) \in R$, the degrees of the terms would need to add to 0. Hence this would give a factorization of the prime p into a product of integers. Since primes in $\mathbb{Z}$ are irreducible, this implies $a(x)$ or $b(x)$ is a unit. Hence $f(x)$ is irreducible in R.

Now suppose $f(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$ of degree at least 1, and constant term ± 1. If $f(x) = a(x)b(x)$ in R, then since $f(x)$ is irreducible in $\mathbb{Q}[x]$, one of $a(x)$ or $b(x)$ is a unit in $\mathbb{Q}[x]$. Say $a(x)$ is a unit. The units in $\mathbb{Q}[x]$ are the nonzero elements of $\mathbb{Q}$. Hence $a(x) \in \mathbb{Q}$. However, since $a(x) \in R$, and $a(x)$ is degree 0, $a(x) \in \mathbb{Z}$. The constant term of $f(x) = \pm 1$, and the constant term of $b(x)$ is an integer, thus $a(x) = \pm 1$. Hence $f(x)$ is irreducible in R.

Now suppose $f(x)$ is an irreducible polynomial in R. If the degree of $f(x)$ is 0, then $f(x)$ must be irreducible in $\mathbb{Z}$, and so $f(x) = \pm p$ for some prime number $p \in \mathbb{Z}$. If the degree of $f(x)$ is at least 1, then its constant term c of $f(x)$ may only be ± 1. Clearly, c cannot be 0 or it would be possible to factor $f(x) = \frac{1}{d}xg(x)$ where d is the denominator of the linear term of $f(x)$, and $g(x) = \frac{df(x)}{x}$. Otherwise, if c were nonzero, then c would not be a unit, and $f(x)$ would factor as $f(x) = c(\frac{1}{c}(f(x) - c) + 1)$ in R.

Suppose the degree of $f(x)$ is at least one, and suppose by way of contradiction that $f(x)$ is reducible in $\mathbb{Q}[x]$ and factors as a product of nonunits $f(x) = a(x)b(x)$. Both of $a(x)$ and $b(x)$ must have nonzero constant terms, call them a_0 and b_0 in $\mathbb{Q}$. Further, $a_0 b_0 = \pm 1$, as seen previously Then $f(x) = a_0 b_0 (\frac{1}{a_0} a(x))(\frac{1}{b_0} b(x))$ is a factorization of $f(x)$ into nonunits. Hence $f(x)$ must be reducible in $f(x)$.

(c) Claim: The element x is not irreducible in R, and cannot be written as a product of irreducibles.

Proof: Since $\frac{1}{2}x$ and 2 are nonunits in R which multiply to x, x is not irreducible in R. However, if we could write $x = p_1(x) \cdots p_n(x)$ for irreducible elements $p_i(x)$, then by the additivity of degrees, all but 1 would have degree 0, and the other, say $p_1(x)$, degree 1. So $p_1(x)$ would be of the form $ax + b$, for $a \in \mathbb{Q}$ and $b = \pm 1$, and for $i > 1$, $p_i(x) = p_i$ would be an irreducible in $\mathbb{Z}$. It is not possible for such polynomials to multiply to a polynomial with 0 constant term, and so x is not a product of irreducible elements of R.

(d) Claim: The element x is not prime in R. $R/(x)$ is not an integral domain in which all nonzero elements which are not units are zero-divisors. Its elements can all be represented uniquely by polynomials of the form $ax + b$ where $a \in [0, 1) \cap \mathbb{Q}$ and $b \in \mathbb{Z}$.

Proof: First, consider the elements 2 and $\frac{1}{2}x$ of R. Neither is contained in (x), since the elements of (x) may only have integer coefficients for their degree 1 term. But $2(\frac{1}{2}x) = x \in (x)$. Hence (x) is not a prime ideal, and x is not prime in R.

In particular, the ring $R/(x)$ is not an integral domain. Two elements $\overline{f(x)}$ and $\overline{g(x)}$ are equal in $R/(x)$ if $f(x) - g(x)$ is a polynomial with no constant term, and whose degree 1 term has an integer coefficient. Therefore every element can be represented uniquely by a polynomial $ax + b$, where $a \in [0, 1) \cap \mathbb{Q}$, and $b \in \mathbb{Z}$. Further, all elements other than ± 1 are zero divisors. This is because if $ax + b \neq \pm 1, 0$, then if $b \neq 0$, $\frac{1}{b}x \notin (x)$ and $\frac{1}{b}x(ax + b) \in (x)$. If $b = 0$, $\frac{1}{2}x(ax) \in (x)$.