Kris Harper
MATH 25800
Homework 3 February 5, 2010

Problem 1 (9.1.4). *Prove that the ideals (x) and (x, y) are prime ideals in $\mathbb{Q}[x, y]$ but only the latter ideal is a maximal ideal.*

Proof. We've seen that $\mathbb{Q}[x, y]/(x, y) \cong \mathbb{Q}$ using the homomorphism $p(x, y) \in \mathbb{Q}[x, y]$ maps to its constant term and the First Isomorphism Theorem. Since $\mathbb{Q}$ is an integral domain, (x, y) must be prime in $\mathbb{Q}[x]$. Furthermore, $\mathbb{Q}[x, y]/(x) = \mathbb{Q}[x][y]/(x) \cong (\mathbb{Q}[x]/(x))[y] \cong \mathbb{Q}[y]$. Since $\mathbb{Q}$ is a field, $\mathbb{Q}[y]$ is an integral domain which means $\mathbb{Q}[x, y]/(x)$ is an integral domain. It follows that (x) must be prime in $\mathbb{Q}[x, y]$.

We see that (x, y) is maximal in $\mathbb{Q}[x, y]$ since $\mathbb{Q}[x, y]/(x, y) \cong \mathbb{Q}$ and $\mathbb{Q}$ is a field. On the other hand, (x) can't be maximal because (x, y) is a proper ideal which contains it. $\square$

Problem 2 (9.1.6). *Prove that (x, y) is not a principal ideal in $\mathbb{Q}[x, y]$.*

Proof. Suppose that $(x, y) = (a(x, y))$ for some polynomial $a(x, y)$. Note that for some polynomial $p(x, y)$, $a(x, y)p(x, y) = x$ and since degrees add when multiplying, we must have that the degree of $a(x, y)$ is either 0 or 1. But $a(x, y)$ can't be constant since there are no constant terms in (x, y). Thus $a(x, y) = px + qy + r$ for some $p, q, r \in \mathbb{Q}$. We still have $a(x, y)p(x, y) = x$ and it follows that the degree of $p(x, y)$ must be 0. It's easy to see that $r = 0$. But this forces $q = 0$ and $p(x, y) = 1/p$. Now it's impossible that $a(x, y)q(x, y) = y$ for some $q(x, y)$ since every term in this product will contain a factor of x. This is a contradiction and so (x, y) can't be principal. $\square$

Problem 3 (9.2.2). *Let F be a finite field of order q and let $f(x)$ be a polynomial in $F[x]$ of degree $n \geq 1$. Prove that $F[x]/(f(x))$ has q^n elements.*

Proof. Let $\overline{g(x)} \in F[x]/(f(x))$. If the degree of $g(x)$ is greater than or equal to n, then write $g(x) = f(x)q(x) + r(x)$ using the division algorithm in $F[x]$ where the degree of $r(x)$ is less than n. Then note that $\overline{g(x)} = \overline{r(x)}$ in $F[x]/(f(x))$ so every polynomial of $F[x]/(f(x))$ can be written as a polynomial of degree less than n. This shows that the polynomials $\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}$ form a basis for the vector space $F[x]/(f(x))$ with coefficients from F. In particular, if F has q elements and every polynomial $\overline{g(x)}$ can be written as a linear combination of $\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}$, then there are only q^n distinct polynomials since there are q choices for each coefficient and n terms. This shows that $F[x]/(f(x))$ has q^n elements. $\square$

Problem 4 (9.2.3). *Let $f(x)$ be a polynomial in $F[x]$. Prove that $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.*

Proof. Note that $f(x)$ being irreducible implies that $f(x)$ is prime since $F[x]$ is a Euclidean Domain and therefore a Principal Ideal Domain. But this also means that $(f(x))$ is prime and therefore maximal. It then follows that $F[x]/(f(x))$ is a field. Conversely, suppose that $F[x]/(f(x))$ is field. Then $(f(x))$ is maximal and thus prime which shows that $f(x)$ is prime and therefore irreducible. $\square$

Problem 5 (9.2.5). *Exhibit* all *the ideals in ring $F[x]/(p(x))$, where F is a field and $p(x)$ is a polynomial in $F[x]$ (describe them in terms of the factorization of $p(x)$).*

Proof. From the fourth Isomorphism Theorem, we know that there is a bijective correspondence between the ideals of $F[x]/(p(x))$ and the ideals of $F[x]$ which contain $(p(x))$. Furthermore, $F[x]$ is a Principal Ideal Domain so all ideals of $F[x]$ containing $(p(x))$ are of the form $(q(x))$ where $q(x) \mid p(x)$. But these are precisely the factors of $p(x)$. So all ideals of $F[x]/(p(x))$ are of the form $(q(x))/(p(x))$ where $q(x)$ is a factor of $p(x)$. In particular, if $p(x)$ is irreducible, then the only ideals of $F[x]/(p(x))$ are $(p(x))/(p(x)) = 0$ and $(1)/(p(x)) = F[x]/(p(x))$, so $F[x]/(p(x))$ is a field as in Problem 4. $\square$

Problem 6 (9.3.4). *Let $R = \mathbb{Z} + x\mathbb{Q}[x] \subseteq \mathbb{Q}[x]$ be the set of polynomials in x with rational coefficients whose constant term is an integer.*
(a) Prove that R is an integral domain and it's units are ± 1.
(b) Show that the irreducibles in R are $\pm p$ where p is a prime in $\mathbb{Z}$ and the polynomials $f(x)$ that are irreducible in $\mathbb{Q}[x]$ and have constant term ± 1. Prove that these irreducibles are prime in R. (c) Show that

x cannot be written as a product of irreducibles in R (in particular, x is not irreducible) and conclude that R is not a U.F.D.
(d) Show that x is not a prime in R and describe the quotient ring $R/(x)$.

Proof. (a) Note that a subring of an integral domain is an integral domain since if two nonzero elements multiply to 0 in the subring, they also multiply to 0 in the ring. Since $\mathbb{Q}[x]$ is a Euclidean Domain, it suffices to prove that R is a subring of $\mathbb{Q}[x]$. This is easily verified as the difference of two polynomials in R will have as a constant term the difference of two integers, also an integer. Likewise, the product of these two polynomials will have as a constant term the product to two integers, also an integer. Thus R is a subring of $\mathbb{Q}[x]$ and also an integral domain.

Additionally, suppose that $p(x)q(x) = 1$. Since degrees add under multiplication, we must have the degree of each $p(x)$ and $q(x)$ is 0 so that they're both integers. But the only units in the integers are ± 1. Thus, these are the only units in R.

(b) Suppose that $p = q(x)q'(x)$ for some prime $p \in \mathbb{Z}$. By the same argument as in part (a), $q(x)$ and $q'(x)$ are both constants which means they're both integers. Therefore p is irreducible in R since it's irreducible in $\mathbb{Z}$. Likewise, it follows that if $f(x)$ with constant term 1 is irreducible in $\mathbb{Q}[x]$ then it's irreducible R. Now suppose $p(x)$ is any polynomial in R which is not of this form. If $p(x)$ is constant, then it's some composite integer and so it factors in R as it factors in $\mathbb{Z}$. Otherwise, suppose $p(x)$ is nonconstant and has a constant term $a \neq \pm 1$. Then $p(x) = aq(x)$ where $q(x)$ has a constant term of ± 1 and coefficients $1/a$ times the coefficients of $p(x)$. Since $a \in \mathbb{Z}$ and is not a unit, $p(x)$ is reducible.

Suppose now that $p(x)$ is an irreducible in R and $p(x) \mid a(x)b(x)$ with $a(x) = \sum_{i=1}^{n} a_i x^i$ and $b(x) = \sum_{i=1}^{m} b_i x^i$. Then there exists $c(x) \in R$ such that $p(x)c(x) = a(x)b(x)$. Suppose first that $p(x) = p$ a prime. Then p divides every coefficient in the product $a(x)b(x)$. In particular, for each $0 \leq k \leq n+m$, p divides $\left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k$ so p divides each term in this sum. Note though that it must be the case that p divides all the a_i or all the b_i because if it doesn't then one of these sums will contain the product $a_i b_j$ for two coefficients which p doesn't divide. Since p is prime in $\mathbb{Z}$, it must divide one of the two, a contradiction.

Now consider the case that $p(x)$ is an irreducible polynomial in $\mathbb{Q}$ with constant term ± 1. Note that the constant terms of $a(x)$ and $b(x)$ must also be ± 1. This then means that $p(x) \mid a(x)$ or $p(x) \mid b(x)$ so $p(x)$ is prime.

(c) This follows directly from part (b). The only irreducibles are primes $\pm p$ and $f(x)$ which has constant term ± 1. A product of two primes will clearly not produce x, and a product of two polynomials with constant terms ± 1 will still have a nonzero constant term. Moreover, a product of p with $f(x)$ will also have a nonzero constant term $\pm p$. Since x is not the product of any pair of irreducibles, it follows readily from induction that x is not the product of any number. It follows that R is not a U.F.D since we can factor x as, for example $2 \cdot (1/2)x$ and $3 \cdot (1/3)x$ where none of the terms involved are not units since they aren't ± 1.

(d) Note that (x) is all the polynomials with rational coefficients which have no constant term and an integer coefficient for x. Then $(2/3x + (x))(3/2x + (x)) = x + (x) = 0$ are two zero divisors in (x), so x can't be prime as the quotient ring isn't an integral domain. The ring $R/(x)$ isn't an integral domain. Polynomials in R are 0 in the quotient ring if and only if they have no constant term and an integer coefficient for x. $\square$