(a) Given $h(x) \in \mathbb{Q}[x]$, show that there are polynomials $a(x), b(x) \in \mathbb{Q}[x]$ satisfying the equation $a(x)f(x) + b(x)g(x) = h(x)$ if and only if $h(x)$ is divisible by $d(x)$.

(b) If $a_0(x), b_0(x) \in \mathbb{Q}[x]$ are particular solutions to the equation in (a), show that the full set of solutions to this equation is given by

$$a(x) = a_0(x) + m(x)\frac{g(x)}{d(x)}$$
$$b(x) = b_0(x) - m(x)\frac{f(x)}{d(x)}$$

as $m(x)$ ranges over the polynomials in $\mathbb{Q}[x]$. [cf. Exercise 4 in Section 8.1]

12. Let $F[x, y_1, y_2, \dots]$ be the polynomial ring in the infinite set of variables $x, y_1, y_2, \dots$ over the field F, and let I be the ideal $(x - y_1^2, y_1 - y_2^2, \dots, y_i - y_{i+1}^2, \dots)$ in this ring. Define R to be the ring $F[x, y_1, y_2, \dots]/I$, so that in R the square of each y_{i+1} is y_i and $y_1^2 = x$ modulo I, i.e., x has a 2^ith root, for every i. Denote the image of y_i in R as $x^{1/2^i}$. Let R_n be the subring of R generated by F and $x^{1/2^n}$.

(a) Prove that $R_1 \subseteq R_2 \subseteq \cdots$ and that R is the union of all R_n, i.e., $R = \cup_{n=1}^{\infty} R_n$.

(b) Prove that R_n is isomorphic to a polynomial ring in one variable over F, so that R_n is a P.I.D. Deduce that R is a Bezout Domain (cf. Exercise 7 in Section 8.2). [First show that the ring $S_n = F[x, y_1, \dots, y_n]/(x - y_1^2, y_1 - y_2^2, \dots, y_{n-1} - y_n^2)$ is isomorphic to the polynomial ring $F[y_n]$. Then show any polynomial relation y_n satisfies in R_n gives a corresponding relation in S_N for some $N \geq n$.]

(c) Prove that the ideal generated by $x, x^{1/2}, x^{1/4}, \dots$ in R is not finitely generated (so R is not a P.I.D.).

13. This exercise introduces a noncommutative ring which is a "right" Euclidean Domain (and a "left" Principal Ideal Domain) but is not a "left" Euclidean Domain (and not a "right" Principal Ideal Domain). Let F be a field of characteristic p in which not every element is a p^{th} power: $F \neq F^p$ (for example the field $F = \mathbb{F}_p(t)$ of rational functions in the variable t with coefficients in $\mathbb{F}_p$ is such a field). Let $R = F\{x\}$ be the "twisted" polynomial ring of polynomials $\sum_{i=0}^{n} a_i x^i$ in x with coefficients in F with the usual (termwise) addition

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$$

but with a noncommutative multiplication defined by

$$\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{k=0}^{n+m}\left(\sum_{i+j=k} a_i b_j^{p^i}\right) x^k .$$

This multiplication arises from defining $xa = a^p x$ for every $a \in F$ (so the powers of x do not commute with the coefficients) and extending in a natural way. Let N be the norm defined by taking the degree of a polynomial in R: $N(f) = \deg(f)$.

(a) Show that $x^k a = a^{p^k} x^k$ for every $a \in F$ and every integer $k \geq 0$ and that R is a ring with this definition of multiplication. [Use the fact that $(a + b)^p = a^p + b^p$ for every $a, b \in F$ since F has characteristic p, so also $(a + b)^{p^k} = a^{p^k} + b^{p^k}$ for every $a, b \in F$.]

(b) Prove that the degree of a product of two elements of R is the sum of the degrees of the elements. Prove that R has no zero divisors.

(c) Prove that R is "right Euclidean" with respect to N, i.e., for any polynomials $f, g \in R$ with $g \neq 0$, there exist polynomials q and r in R with

$$f = qg + r \qquad \text{with } r = 0 \text{ or } \deg(r) < \deg(g).$$

Use this to prove that every *left* ideal of R is principal.

(d) Let $f = \theta x$ for some $\theta \in F$, $\theta \notin F^p$ and let $g = x$. Prove that there are no polynomials q and r in R with

$$f = gq + r \qquad \text{with } r = 0 \text{ or } \deg(r) < \deg(g),$$

so in particular R is not "left Euclidean" with respect to N. Prove that the right ideal of R generated by x and θx is not principal. Conclude that R is not "left Euclidean" with respect to *any* norm.

9.3 POLYNOMIAL RINGS THAT ARE UNIQUE FACTORIZATION DOMAINS

We have seen in Proposition 1 that if R is an integral domain then $R[x]$ is also an integral domain. Also, such an R can be embedded in its field of fractions F (Theorem 15, Section 7.5), so that $R[x] \subseteq F[x]$ is a subring, and $F[x]$ is a Euclidean Domain (hence a Principal Ideal Domain and a Unique Factorization Domain). Many computations for $R[x]$ may be accomplished in $F[x]$ at the expense of allowing fractional coefficients. This raises the immediate question of how computations (such as factorizations of polynomials) in $F[x]$ can be used to give information in $R[x]$.

For instance, suppose $p(x)$ is a polynomial in $R[x]$. Since $F[x]$ is a Unique Factorization Domain we can factor $p(x)$ uniquely into a product of irreducibles in $F[x]$. It is natural to ask whether we can do the same in $R[x]$, i.e., is $R[x]$ a Unique Factorization Domain? In general the answer is no because if $R[x]$ were a Unique Factorization Domain, the constant polynomials would have to be uniquely factored into irreducible elements of $R[x]$, necessarily of degree 0 since the degrees of products add, that is, R would itself have to be a Unique Factorization Domain. Thus if R is an integral domain which is not a Unique Factorization Domain, $R[x]$ cannot be a Unique Factorization Domain. On the other hand, it turns out that if R is a Unique Factorization Domain, then $R[x]$ is also a Unique Factorization Domain. The method of proving this is to first factor uniquely in $F[x]$ and then "clear denominators" to obtain a unique factorization in $R[x]$. The first step in making this precise is to compare the factorization of a polynomial in $F[x]$ to a factorization in $R[x]$.

Proposition 5. *(Gauss' Lemma)* Let R be a Unique Factorization Domain with field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for some nonconstant polynomials $A(x), B(x) \in F[x]$, then there are nonzero elements $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both lie in $R[x]$ and $p(x) = a(x)b(x)$ is a factorization in $R[x]$.

Proof: The coefficients of the polynomials on the right hand side of the equation $p(x) = A(x)B(x)$ are elements in the field F, hence are quotients of elements from the Unique Factorization Domain R. Multiplying through by a common denominator for all these coefficients, we obtain an equation $dp(x) = a'(x)b'(x)$ where now $a'(x)$ and $b'(x)$ are elements of $R[x]$ and d is a nonzero element of R. If d is a unit in R, the proposition is true with $a(x) = d^{-1}a'(x)$ and $b(x) = b'(x)$. Assume d is not a unit and write d as a product of irreducibles in R, say $d = p_1 \cdots p_n$. Since p_1 is irreducible in R, the ideal (p_1) is prime (cf. Proposition 12, Section 8.3), so by Proposition 2 above, the ideal $p_1R[x]$ is prime in $R[x]$ and $(R/p_1R)[x]$ is an integral domain. Reducing the equation $dp(x) = a'(x)b'(x)$ modulo p_1, we obtain the equation $0 = \overline{a'(x)}\ \overline{b'(x)}$ in this integral domain (the bars denote the images of these polynomials in the quotient ring), hence one of the two factors, say $\overline{a'(x)}$ must be 0. But this means all the coefficients of $a'(x)$ are divisible by p_1, so that $\frac{1}{p_1}a'(x)$ also has coefficients in R. In other words, in the equation $dp(x) = a'(x)b'(x)$ we can cancel a factor of p_1 from d (on the left) and from either $a'(x)$ or $b'(x)$ (on the right) and still have an equation in $R[x]$. But now the factor d on the left hand side has one fewer irreducible factors. Proceeding in the same fashion with each of the remaining factors of d, we can cancel all of the factors of d into the two polynomials on the right hand side, leaving an equation $p(x) = a(x)b(x)$ with $a(x), b(x) \in R[x]$ and with $a(x), b(x)$ being F-multiples of $A(x), B(x)$, respectively. This completes the proof.

Note that we cannot prove that $a(x)$ and $b(x)$ are necessarily R-multiples of $A(x)$, $B(x)$, respectively, because, for example, we could factor x^2 in $\mathbb{Q}[x]$ with $A(x) = 2x$ and $B(x) = \frac{1}{2}x$ but no *integer* multiples of $A(x)$ and $B(x)$ give a factorization of x^2 in $\mathbb{Z}[x]$.

The elements of the ring R become *units* in the Unique Factorization Domain $F[x]$ (the units in $F[x]$ being the nonzero elements of F). For example, $7x$ factors in $\mathbb{Z}[x]$ into a product of two irreducibles: 7 and x (so $7x$ is not irreducible in $\mathbb{Z}[x]$), whereas $7x$ is the unit 7 times the irreducible x in $\mathbb{Q}[x]$ (so $7x$ is irreducible in $\mathbb{Q}[x]$). The following corollary shows that this is essentially the *only* difference between the irreducible elements in $R[x]$ and those in $F[x]$.

Corollary 6. Let R be a Unique Factorization Domain, let F be its field of fractions and let $p(x) \in R[x]$. Suppose the greatest common divisor of the coefficients of $p(x)$ is 1. Then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$. In particular, if $p(x)$ is a monic polynomial that is irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$.

Proof: By Gauss' Lemma above, if $p(x)$ is reducible in $F[x]$, then it is reducible in $R[x]$. Conversely, the assumption on the greatest common divisor of the coefficients of $p(x)$ implies that if it is reducible in $R[x]$, then $p(x) = a(x)b(x)$ where neither $a(x)$ nor $b(x)$ are constant polynomials in $R[x]$. This same factorization shows that $p(x)$ is reducible in $F[x]$, completing the proof.

Theorem 7. R is a Unique Factorization Domain if and only if $R[x]$ is a Unique Factorization Domain.

Proof: We have indicated above that $R[x]$ a Unique Factorization Domain forces R to be a Unique Factorization Domain. Suppose conversely that R is a Unique Factorization Domain, F is its field of fractions and $p(x)$ is a nonzero element of $R[x]$. Let d be