Exercises from Chapter 9

Wesley Basener

May 31, 2025

Problem 1.1. Let $p(x,y,z) = 2x^2y - 3xy^3z + 4y^2z^5$ and $q(x,y,z) = 7x^2 + 5x^2y^3z^4 - 3x^2z^3$ be polynomials in $\mathbb{Z}[x,y,z]$.

(a) Write each p and q as a polynomial in x with coefficients in $\mathbb{Z}[y,z]$.

(b) Find the degree of each of p and q.

(c) Find the degree of p and q in each of the three variables x, y, and z.

(d) Compute pq and find the degree of pq in each of the three variables x, y, and z.

(e) Write pq as a polynomial in the variable z with coefficients in $\mathbb{Z}[x,y]$

Proof. For part a, $p = (2y)x^2 - (3y^3z)x + (4y^2z^5)x^0$ and $q = (7 + 5y^3z^4 - 3z^3)x^2$. For part b, the degree of p is the degree of the last term $2 + 5 = 7$ and the degree of q is the degree of the center second term $2 + 3 + 4 = 9$. For part c, x, y, z degrees of p are $2, 3$,and 5 respectively and for q they are $2, 3$, and 4 respectively. For part d,

$$pq = (2x^2y - 3xy^3z + 4y^2z^5)(7x^2 + 5x^2y^3z^4 - 3x^2z^3)$$

$$= 14x^4y - 21x^3y^3z - 6x^4yz^3 + 9x^3y^3z^4 + 10x^4y^4z^4 + 28x^2y^2z^5 - 15x^3y^6z^5 - 12x^2y^2z^8 + 20x^2y^5z^9$$

The degrees of x, y, and z are $4, 6$, and 9 respectively. Lastly, for part e, we have

$$(20x^2y^5)z^9 - (12x^2y^2)z^8 + (28x^2y^2 - 15x^3y^6)z^5 + (9x^3y^3 + 10x^4y^4)z^4 - (6x^4y)z^3 - (21x^3y^3)z + (14x^4y)z^0$$

□

Problem 1.2. Repeat the preceding exercise under the assumption that the coefficients are of p and q are in $\mathbb{Z}/3\mathbb{Z}$.

Proof. We can start by rewriting p and q's coefficients in $\mathbb{Z}/3\mathbb{Z}$.

$$p = 2x^2y + y^2z^5 \text{ and } q = x^2 + 2x^2y^3z^4$$

For part a, we have $p = (2y)x^2 + (y^2z^5)x^0$ and $q = (1 + 3y^3z^4)x^2$. For part b, the degree of p is 7 and the degree of q is 9. For part c, the degree of p in x, y, and z is $2, 2$, and 5 respectively and for q it is $2, 3$, and 4 respectively. For part d,

$$pq = 2x^4y + x^4y^4z^4 + x^2y^2z^5 + 2x^2y^5z^9$$

The degrees of pq in x, y, and z are $4, 6$, and 9 respectively. Finally, for part e,

$$pq = (2x^2y^5)z^9 + (x^2y^2)z^5 + (x^4y^4)z^4 + (2x^4y)z^0$$

□

Problem 1.3. If R is a commutative ring and and $x_1, x_2, ..., x_n$ are independent variables over R, prove that $R[x_{\pi(1)}, x_{\pi(2)}, ..., x_{\pi(n)}]$ is isomorphic to $R[x_1, x_2, ..., x_n]$ for any permutation of $\{1, 2, ..., n\}$.

Proof. Any element of $R[x_1, x_2, ..., x_n]$ will have the form

$$\alpha = (\Sigma_{i_1=0}^{m}(\Sigma_{i_2=0}^{m}...(\Sigma_{i_n=0}^{m}\alpha_{i_1,i_2,...,i_n}x_1^{i_1}x_2^{i_2}...x_n^{i_n})...))$$

Let α and β be two such polynomials and let $\phi : R[x_1, x_2, ..., x_n] \to R[x_{\pi(1)}, x_{\pi(2)}, ..., x_{\pi(n)}]$ be the variable permutation function. Then, for addition,

$$\phi(\alpha) + \phi(\beta) =$$

$$\phi((\Sigma_{i_1=0}^{m}(\Sigma_{i_2=0}^{m}...(\Sigma_{i_n=0}^{m}\alpha_{i_1,i_2,...,i_n}x_1^{i_1}x_2^{i_2}...x_n^{i_n})...))) + \phi((\Sigma_{i_1=0}^{m}(\Sigma_{i_2=0}^{m}...(\Sigma_{i_n=0}^{m}\beta i_1, i_2, ..., i_n x_1^{i_1}x_2^{i_2}...x_n^{i_n})...)) =$$

$$\phi((\Sigma_{i_1=0}^{m}(\Sigma_{i_2=0}^{m}...(\Sigma_{i_n=0}^{m}\alpha_{i_1,i_2,...,i_n}x_{\pi(1)}^{i_1}x_{\pi(2)}^{i_2}...x_{\pi(n)}^{i_n})...))) + \phi((\Sigma_{i_1=0}^{m}(\Sigma_{i_2=0}^{m}...(\Sigma_{i_n=0}^{m}\beta i_1, i_2, ..., i_n x_{\pi(1)}^{i_1}x_{\pi(2)}^{i_2}...x_{\pi(n)}^{i_n})...))) =$$

$$\phi((\Sigma_{i_1=0}^{m}(\Sigma_{i_2=0}^{m}...(\Sigma_{i_n=0}^{m}(\alpha_{i_1,i_2,...,i_n} + \beta i_1, i_2, ..., i_n)x_{\pi(1)}^{i_1}x_{\pi(2)}^{i_2}...x_{\pi(n)}^{i_n})...))) =$$

$$\phi(\alpha + \beta)$$

Hence, the function satisfies the homomorphism condition on addition.

For multiplication, the coefficient of the term $x_1^{i_1}x_2^{i_2}...x_n^{i_n}$ in $\phi(\alpha \cdot \beta)$ will be the sum of all $\alpha_{k_1,k_2,...,k_n} \cdot \beta_{j_1,j_2,...,j_n}$ where $k_1 + j_1 = i_{\pi^{-1}(1)}, k_2 + j_2 = i_{\pi^{-1}(2)}, ..., k_n + j_n = i_{\pi^{-1}(n)}$ are all true. The coefficients of the $x_1^{i_1}x_2^{i_2}...x_n^{i_n}$ term in $\phi(\alpha) \cdot \phi(\beta)$ will be the sum of all $\alpha_{k_1,k_2,...,k_n} \cdot \beta_{j_1,j_2,...,j_n}$ where $k_{\pi(1)} + j_{\pi(1)} = i_1, k_{\pi(2)} + j_{\pi(2)} = i_2, ..., k_{\pi(n)} + j_{\pi(n)} = i_n$ are all true. But $k_{\pi(l)} + j_{\pi(l)} = i_l$ is true for all l in $[n]$ if and only if $k_l + j_l = i_{\pi^{-1}(l)}$ is also true for all l in $[n]$. So $\phi(\alpha \cdot \beta)$ and $\phi(\alpha) \cdot \phi(\beta)$ have precisely the same coefficients.

Since the set of units in $R[x_1, x_2, ..., x_n]$ are the set of units in R, and ϕ is the identity element on R, $\phi(1_{R[x_1,x_2,...,x_n]}) = 1_{R[x_1,x_2,...,x_n]}$.

These three cases prove that ϕ is a homomorphism on $R[x_1, x_2, ..., x_n]$. To show that it is an isomorphism, notice first that for r in R, $\phi(rx_1^{i_1}x_2^{i_2}...x_n^{i_n}) = rx_{\pi(1)}^{i_1}x_{\pi(2)}^{i_2}...x_{\pi(n)}^{i_n}$ is nonzero if and only if r is nonzero. Second, recall that ϕ is the identity function on R. Hence, the inverse of the kernal of ϕ is the 0 element of R. Therefore, ϕ is an isomorphism. □

Problem 1.4. Prove that the ideals (x) and (x, y) are prime ideals in $\mathbb{Q}[x, y]$ but only the later ideal is maximal.

Proof. If the second ideal were not prime, then there would exist a, b in R such that $ab = cx^n y^m$ for nonzero c in R. But this would violate the closure of R under multiplication, because $cx^n y^m$ is not in R. Thus, (x, y) is prime. The same result follows for the first ideal (x) by letting a, b, and c be in $R[y]$.

Since $(x) \subset (x, y)$, (x) is not maximal. For any $\alpha = \Sigma_{i=0,j=0}^{n,m}\alpha_{i,j}x^i y^j$, α is not in (x, y) if and only if $\alpha_{0,0} \neq 0$. For every such α, $(x, y) + (\alpha) = (\alpha_{0,0}) = (1) = \mathbb{Q}[x, y]$. So the only ideal containing (x, y) is $\mathbb{Q}[x, y]$. Hence, (x, y) is maximal.

□

Problem 1.5. Prove that (x, y) and $(2, x, y)$ are prime ideals in $\mathbb{Z}[x, y]$ but only the latter ideal is a maximal ideal.

Proof. There are no elements not equal to x, y, or 2 in $\mathbb{Z}[x,y]$ that multiply to equal x, y, or 2 respectively. So the ideals generated by these elements are prime.

Since $(x,y) \subset (2,x,y) \subset \mathbb{Z}[x,y]$, where all containment is proper, (x,y) is not maximal. For any polynomial $\alpha = \Sigma_{i=0,j=0}^{m,n} \alpha_{i,j} x^i y^j$ is not in $(2,x,y)$ if and only if $\alpha_{0,0}$ is not zero and is not divisible by 2. This means that there are a, b in $\mathbb{Z}$ such that $a\alpha_{0,0} + b2 = 1$. Hence, $(2,x,y) + (\alpha) = \mathbb{Z}[x,y]$. So there are no ideals containing $(2,x,y)$ aside from $\mathbb{Z}[x,y]$. Therefore, $(2,x,y)$ is a maximal ideal. □

Problem 1.6. Prove that (x,y) is not principle in $\mathbb{Q}[x,y]$.

Proof. The gcd of x and y is 1. So, the only element that could generate (x,y) is 1, which would also generate the rest of $\mathbb{Q}[x,y]$. □

Problem 1.7. Let R be a commutative ring with 1. Prove that a polynomial ring in more than one variable over R is not a PID.

Proof. For any $R[x,y]$, the ideal (x,y) is not principle. By induction, this is true for any polynomial ring with more than one variable. □

Problem 1.8. Let F be a field and $R = F[x, x^2y, x^3y^2, ..., x^n y^{n-1}, ...]$ be a subring of the polynomial ring $F[x,y]$.

(a) Prove that the fields of fractions of R and $F[x,y]$ are the same.

(b) Prove that R contains an ideal that is not finitely generated.

Proof. For any f in the field F, $fx \cdot 1/x = f$ is in the fraction field of R and so are $x^2y \cdot 1/x^2 = y$ and x. Therfore, the fraction field is $(F,x,y) = F[x,y]$.

For part b, consider the ideal of elements $fx^m y^n$, where $m > n+1$. Suppose $x^{m+2}y^m$, which is indeed part of the ideal, is not a generator of the ideal. Then this element must be divisible by an element of the ideal. This is impossible because there is no partition a_1, b_1 and $a_2, b2$ of the integers $m+2, m$ such that $a_1 > b_1 + 1$ and $a_2 > b_2$. Therefore, the ideal is not finitely generated. □

Problem 1.9. Prove that a polynomial ring in infinitely many variables with coefficients in any commutative ring contains ideals that are not finitely generated.

Proof. In $R[x_1, x_2, ...]$, the ideal of all elements containing variables is not finitely generated, every variable x_i by itself is in the ideal, but is not divisible by other variables. □

Problem 1.10. Prove that the ring $\mathbb{Z}[x_1, x_2, x_3, ...]/(x_1x_2, x_3x_4, x_5x_6, ...)$ contains infinitely many minimal prime ideals.

Proof. Consider the ideal $(x_{\beta_1}, x_{\beta_2}, ...)$, where β_1 is either 1 or 2, β_2 is either 3 or 4 and so on. This is a prime ideal, since each of its generators are prime. It contains the 0 ideal of the quotient $(x_1x_2, x_3x_4, x_5x_6, ...)$. And, removing any of its generators would keep it from containing the 0 ideal, so it is minimal. Since there are infinite possibilities of the combinations of βs, there are infinite such minimal ideals in the ring. □

Problem 1.11. Show that the radical of the ideal $I = (x, y^2)$ in $\mathbb{Q}[x,y]$ is (x,y). Deduce that I is a primary ideal that is not a power of a prime ideal.

Proof. The radical of I is the ideal formed by the square root of all elements in I, if the square root exists. The only elements that have a square root in I are of the form q^2x^{2n}, q^2y^{2n}, and $q^2x^{2m}y^{2n}$. The square root of these elements is qx^n, qy^n, and qx^my^n, which is obviously generated by the elements x, y. Hence, $\text{rad}(I) = (x,y)$

The above works to show (x,y) is any root of I. Simply replace 2 with any other natural number > 0. Therefore, I, which is obviously primary, is not the power of any prime ideal. □

Problem 1.12. Let $R = \mathbb{Q}[x,y,z]$ and let bars denote passage to $\mathbb{Q}[x,y,z]/(xy - z^2)$. Prove that $\overline{P} = (\overline{x}, \overline{y})$ is a prime ideal. Show that $\overline{xy} \in \overline{P}^2$ but that no power (This shows that $\overline{P}$ is a prime ideal whose square is not a primary ideal).

Proof. Since (x, y) is prime in $\mathbb{Q}[x, y, z]$, it is prime in $\mathbb{Q}[x, y, z]/(xy - z^2)$. Hence, $\overline{P}$ is a prime ideal.

In $\mathbb{Q}[x, y, z]/(xy - z^2)$, xy is equivalent to z^2. This can be seen by noticing that in $\mathbb{Q}[x, y, z]/(xy - z^2)$, $xy = xy + (-1) \cdot (xy - z^2) = xy - xy + z^2 = z^2$. Hence, $\overline{xy}$ is in $\overline{P}^2$.

To see that no power of y is in $\overline{P}^2$, we consider the quotient ring definition of $\overline{y}^n$, which is $y^n + (xy - z^2)$. We want to show that no element of the ideal $(xy - z^2)$ adds to y^n to create an element of $\overline{P}^2$. Suppose this is not true, then there must be some a in $\mathbb{Q}[x, y, z]/(xy - z^2)$ where $y^n + a(xy - z^2) \in \overline{P}^2 = (x^2, z^2)$. This would require either axy or az^2 to cancel y^n, which is not possible. So, there is no such a. Hence, no power of y is in $\overline{P}^2$. □

Problem 1.13. Prove that the rings $F[x, y]/(y^2 - x)$ and $F[x, y]/(y^2 - x^2)$ are not isomorphic for any field F.

Proof. For brevity, denote $F[x, y]/(y^2 - x)$ as A and $F[x, y]/(y^2 - x^2)$ as B.

Notice that $y^2 - x^2 = (y - x) \cdot (y + x)$. Since neither $(y - x)$ nor $(y + x)$ are in $(y^2 - x^2)$, $(y^2 - x^2)$ is not prime. So, B has zero divisors and is not an integral domain. $(y^2 - x)$ however is prime (see exercise 1.14 below). So A has no zero divisors and is an integral domain.

Suppose there is an isomorphism $\phi : B \to A$. Then since $(y - x) \cdot (y + x)$ is in the kernel of B, $\phi((y - x) \cdot (y + x))$ must be in the kernel of A. However $\phi((y - x) \cdot (y + x)) = \phi(y - x) \cdot \phi(x + y)$ is also in the kernel of A.

But since ϕ is an isomorphism and neither $(y - x)$ nor $(y + x)$ are in the kernel of B, neither $\phi((y - x))$ nor $\phi((y + x))$ can be in the kernel of A. This implies that A is not an integral domain, contradicting our earlier results. Therefore, such an isomorphism cannot exist, regardless of the field F. □

Problem 1.14. Let R be an integral domain and let i, j be relatively prime integers. Prove that the ideal $(x^i - y^j)$ is a prime ideal in $R[x, y]$. [Consider the ring homomorphism ϕ from $R[x, y]$ to $R[t]$ defined by mapping x to t^j and mapping y to t^i. Show that an element of $R[x, y]$ differs from an element in $(x^i - y^j)$ by a polynomial $f(x)$ of degree at most $j - 1$ in y and observe that the exponents of $\phi(x^r y^s)$ are distinct for $0 \leq s < j$.]

Proof. The kernel of the homomorphism ϕ is the ideal $(x^i - y^j)$. To see this, notice that

$$\phi(\Sigma_{k=1}^{n} a_k x^{r_k} y^{s_k}) = \phi(\Sigma_{k=1}^{n} a_k t^{j \cdot r_k + i \cdot s_k})$$

Suppose $\Sigma_{k=1}^{n} a_k x^{r_k} y^{s_k}$ is in the kernel of ϕ. In order to cancel in $R[t]$, this polynomial must be the sum of components whose images are homogeneous in $R[t]$. Let $\Sigma_{k=1}^{m} a_k x^{r_k} y^{s_k}$ be one such component.

$\phi(x^{2i} - x^i y^j) = t^{2ij} - t^{ij+ij}$ □

Problem 1.15. Let $p(x_1, x_2, ..., x_n)$ be a homogeneous polynomial of degree k in $R[x_1, ..., x_n]$ Prove that for all $\lambda \in R$ we have $p(\lambda x_1, \lambda x_2, ..., \lambda x_n) = \lambda^k p(x_1, x_2, ..., x_n)$.

Proof. The homogeneous polynomial can be written as the sum $\Sigma_{i=0}^{k} r_i x_1^{e_{i,1}} x_2^{e_{i,2}} ... x_n^{e_{i,n}}$ where $e_{i,1} + e_{i,2} + ... + e_{i,n} = k$ for all i. The polynomial $p(\lambda x_1, \lambda x_2, ..., \lambda x_n)$ can be similarly written by substituting λx_i for each x_i which lends

$$\Sigma_{i=0}^{k} r_i (\lambda x_1)^{e_{i,1}} (\lambda x_2)^{e_{i,2}} ... (\lambda x_n)^{e_{i,n}} = \Sigma_{i=0}^{k} \lambda^{e_{i,1} + e_{i,2} + ... + e_{i,n}} r_i x_1^{e_{i,1}} x_2^{e_{i,2}} ... x_n^{e_{i,n}}.$$

Since the exponents sum to k, we have

$$\Sigma_{i=0}^{k} \lambda^k r_i x_1^{e_{i,1}} x_2^{e_{i,2}} ... x_n^{e_{i,n}} = \lambda^k \Sigma_{i=0}^{k} r_i x_1^{e_{i,1}} x_2^{e_{i,2}} ... x_n^{e_{i,n}} = \lambda^k p(x_1, x_2, ..., x_n).$$

□

Problem 1.16. prove that the product of two homogeneous polynomials is again homogeneous.

Proof. In $R[x_1, ..., x_n]$, two homogeneous polynomials of degree k and m can be written as the sum $\Sigma_{i=0}^{k} a_i x_1^{e_{i,1}} x_2^{e_{i,2}} ... x_n^{e_{i,n}}$ and $\Sigma_{i=0}^{k} b_i x_1^{l_{i,1}} x_2^{l_{i,2}} ... x_n^{l_{i,n}}$ where b_i and a_i are in R, $e_{i,1} + e_{i,2} + ... + e_{i,n} = k$ and $l_{i,1} + l_{i,2} + ... + l_{i,n} = m$ for all i. Multiplying These polynomials lends

$$(\Sigma_{i=0}^{k} a_i x_1^{e_{i,1}} x_2^{e_{i,2}} ... x_n^{e_{i,n}}) \cdot (\Sigma_{i=0}^{k} b_i x_1^{l_{i,1}} x_2^{l_{i,2}} ... x_n^{l_{i,n}}) = \Sigma_{i=0}^{k} \Sigma_{j=0}^{k} (a_i x_1^{e_{i,1}} x_2^{e_{i,2}} ... x_n^{e_{i,n}}) \cdot (b_j x_1^{l_{j,1}} x_2^{l_{j,2}} ... x_n^{l_{j,n}}))$$

$$= \Sigma_{i=0}^{k} \Sigma_{j=0}^{k} (a_i x_1^{e_{i,1}} x_2^{e_{i,2}} ... x_n^{e_{i,n}}) \cdot (b_j x_1^{l_{j,1}} x_2^{l_{j,2}} ... x_n^{l_{j,n}})) = \Sigma_{i=0}^{k} \Sigma_{j=0}^{k} a_i b_j x_1^{e_{i,1}+l_{j,1}} x_2^{e_{i,2}+l_{i,2}} ... x_n^{e_{i,n}+l_{j,n}})$$

Each term in this polynomial has degree $e_{i,1} + l_{i,1} + e_{i,2} + l_{i,2} + ... + e_{i,n} + l_{i,n}$ by the distributive rule, this is becomes $k + m$. So the product is homogeneous with degree $k + m$. □

Problem 1.17. An ideal I in $R[x_1, ..., x_n]$ is called a homogeneous ideal if whenever $p \in I$ then each homogeneous component of p is also in I. Prove that an ideal is a homogeneous if and only if it may be generated by homogeneous polynomials. [use induction on degrees to show the "if" implication.]

Proof. Let I be a homogeneous ideal in $R[x_1, ..., x_n]$. Then the generators of I must each be homogeneous. Otherwise, there would be some non-homogeneous generator p in I.

Let I be an ideal generated by homogeneous polynomials. By the previous exercise, we know the product of two homogeneous polynomials is also homogeneous. The sum of homogeneous polynomials might not be homogeneous, but it will be the sum of homogeneous components, each of which will be in p. So the desired property holds on operations within the ideal.

To see that the property holds on multiplication of elements outside the ideal, let $p \cdot \Sigma_{i=0}^{n} a_i x_1^{e_{i,1}} x_2^{e_{i,2}} ... x_n^{e_{i,n}}$ be any polynomial in I, where the term in the sum is not by itself in I but p is some combination of the generators. We can distribute the p, lending $\Sigma_{i=0}^{n} p \cdot a_i x_1^{e_{i,1}} x_2^{e_{i,2}} ... x_n^{e_{i,n}}$. The polynomial is now the sum of of the terms $p \cdot a_i x_1^{e_{i,1}} x_2^{e_{i,2}} ... x_n^{e_{i,n}}$, each of which have the desired property. □

Problem 1.18. Let R be an arbitrary ring and let Func(R) be the ring of all functions from R to itself. If $p(x) \in R[x]$ is a polynomial, let $f_p \in$ Func(R) be thr

Problem 2.1. Let $f(x) \in F[x]$ be a polynomial of degree $n \geq 1$ and let bars denote passage to the quotient $F[x]/(f(x))$. Prove that for each $\overline{g(x)}$ there is a unique polynomial $g_0(x)$ of degree $\leq n - 1$ such that $\overline{g(x)} = \overline{g_0(x)}$ (equivalently, the elements $\overline{1}, \overline{x}, ..., \overline{x^{n-1}}$) are a basis of the vector space $F[x]/(f(x))$ over F - in particular, the dimension of this space is n). [Use the Division Algorithm.]

Proof. Since F is a field, we have by Theorem 3 that $F[x]$ is a Euclidean domain. So, for $g(x)$ and $f(x)$, there must be unique polynomials $q(x)$ and $r(x)$ where $\deg(r(x)) < \deg(f(x))$.

$$g(x) = f(x) \cdot q(x) + r(x)$$

Since the term $f(x) \cdot q(x)$ is obviously in the ideal $(f(x))$, we can conclude that $\overline{(g(x))} = \overline{r(x)}$. The polynomial $r(x)$ therefore fulfills the desired properties. □

Problem 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. [Use preceding exercise.]

Proof. From the preceding exercise, we know that every element of $p(x) \in F[x]$ has a unique polynomial $r(x)$ such that $\overline{p(x)} = \overline{r(x)}$ and $\deg(r(x)) < n$. Since every such polynomial is unique, no two polynomials of degree $< n$ are equal in $F[x]/(f(x))$. Therefore, there is an bijection between $F[x]/(f(x))$ and polynomials of degree $< n$.

Let $p(x)$ be a polynomial of degree $< n$. From the preceding paragraph, we can conclude that the number of choices for $p(x)$ is the order of $F[x]$. Since F is a finite field of order q, there are q choices for each coefficient in the $p(x)$. Since there are n possible terms in $p(x)$, there are q^n possible choices for $p(x)$ Therefore, the order of $F[x]$ is p^n. □

Problem 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. [Use proposition 7, section 8.2].

Proof. By theorem 3 of section 9.2, $F[x]$ is a Euclidean domain. So, $f(x)$ is irreducible if and only if its gcd with every element in $F[x]$ is 1. This is true if and only if for any $g(x)$ in $F[x]$, there exists $a(x)$ and $b(x)$ in $F[x]$ such that $a(x)g(x) + b(x)f(x) = 1$. Consider $g(x)$'s passage to $F[x]/(f(x))$, which can be written $g(x)+(f(x))$. Multiplying by $a(x)+(f(x))$ lends $a(x)g(x)+(f(x))$. Since $b(x)f(x) \in (f(x))$, the set $a(x)g(x)+(f(x))$ contains the unity element of $F[x]$ and is therefore the unity element of $F[x]/(f(x))$. We can conclude that $g(x)+(f(x))$ is a unit in $F[x]/(f(x))$. Since $g(x)$ is arbitrary, every element of $F[x]/(f(x))$ has multiplicative inverse if and only $f(x)$ is irreducible, which of course is true if and only if $F[x]/(f(x))$ is a field. □

Problem 2.4. Let F be a finite field. Prove that $F[x]$ contains infinitely many primes.

Proof. First note that every finite field has unity 1 and $1 + x$ is prime. Hence, every polynomial ring over a finite field has at least one prime.

Suppose for the sake of contradiction that there are only finite primes. Then we can enumerate the finite number of polynomials as $p_0(x), p_1(x), ..., p_n(x)$. Consider the product of all these polynomials plus one, $p_0(x) \cdot p_1(x) \cdot ... \cdot p_n(x) + 1$. This product is outside of our set of primes and is by assumption is not prime. So, it must be divisible by at least two primes. This implies that 1 is divisible by a prime, which is a contradiction. □

Problem 2.5. Exhibit all the ideals of the ring $F[x]/(p(x))$, where F is a field and $p(x)$ is a polynomial in $F[x]$. (describe them in terms of factorizing $p(x)$).

Proof. Let bars denote passage from $F[x]$ to $F[x]/p(x)$. Clearly, we have the trivial ideals $(\overline{1})$ and $(\overline{0})$. From corollary 4, $F[x]/(p(x))$ is a PID, so any ideal will have a single generator. Suppose $\overline{q(x)}$ is a generator for a non trivial ideal in $F[x]/(p(x))$, if one exists. We can rewrite $(\overline{q(x)})$ as the set $(q(x)) + (p(x))$.

By Bezout's lemma, the gcd of $q(x)$ and $p(x)$ must be in the ideal and in fact generates the ideal. Since we are assuming the ideal is non trivial, the gcd cannot be 1. Hence $q(x)$ and $p(x)$ are not mutually prime. Since $\gcd(q(x), p(x)) = \gcd(\gcd(q(x), p(x)), p(x))$, we can stipulate that $q(x)$ divides $p(x)$ without loss of generality. Therefore, all ideals in $F[x]/p(x)$ are generated by elements $q(x) \neq 1$ such that $q(x)|p(x)$.

More precisely, if $p(x)$ has prime decomposition $p(x) = p_0(x) \cdot p_1(x) \cdot ... \cdot p_n(x)$, then all ideals in $F[x]/(p(x))$ have the form $(\bigcap_{i \in K} p_i(x))$ where K is some properly contained nonempty subset of $[0, n]$. □

Problem 2.11. Suppose $f(x)$ and $g(x)$ are two nonzero polynomials in $\mathbb{Q}[x]$ with greatest common divisor $d(x)$.

(a) Given $h(x) \in \mathbb{Q}$ show that there are two polynomials $a(x), b(x) \in \mathbb{Q}$ 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 $\mathbb{Q}[x]$.

Proof. **(a)** For the forward implication, since $d(x)$ is the gcd of $f(x)$ and $g(x)$, there exists polynomials $f'(x)$ and $g'(x)$ such that $f'(x)d(x) = f(x)$ and $g'(x)d(x) = g(x)$. We can use this to decompose the equation

$$h(x) = a(x)f(x) + b(x)g(x) = a(x)f'(x)d(x) + b(x)g'(x)d(x) = d(x) \cdot (a(x)f'(x) + b(x)g'(x))$$

Clearly, the right side of the equation is divisible by $d(x)$. Hence, so is $h(x)$.

For the backward implication, recall that $\mathbb{Q}[x]$ is a Euclidean domain. So, by Bezout's lemma, there exists two polynomials $a'(x), b'(x)$ such that $a'(x)f(x) + b'(x)g(x) = d(x)$. For any $h(x)$ divisible by $d(x)$, there exists some $h'(x)$ such that $h(x) = h'(x)d(x)$. We can use this to rewrite $h(x)$ as

$$h(x) = h'(x)d(x) = h'(x)(a'(x)f(x) + b'(x)g(x)) = (h'(x)a'(x))f(x) + (h'(x)b'(x))g(x)$$

Hence, for any $h(x)$ divisible by $d(x)$, $h(x)$ setting $a(x) = a'(x)h'(x)$ and $b(x) = b'(x)h'(x)$ gives the desired equation. □

Proof. **(b)** We will first show that any solution to the equation has such a form. Then we need to show that any choice for $m(x)$ will garner such a solution.

Suppose that $a(x), b(x)$ are any solution to the equation. We have

$$a_0(x)f(x) + b_0(x)g(x) = h(x) = a(x)f(x) + b(x)g(x)$$

Which lends

$$a(x)f(x) - a_0(x)f(x) = b_0(x)g(x) - b(x)g(x)$$

Factoring out $f(x)$ and $g(x)$ leads to

$$f(x)(a(x) - a_0(x)) = g(x)(b_0(x) - b(x))$$

This implies that $(a(x) - a_0(x))|\frac{g(x)}{d(x)}$ $(b_0(x) - b(x))|\frac{f(x)}{d(x)}$. Hence there are some polynomials $m(x), n(x)$ such that

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

We can rewrite the above as

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

We now need only show that $m(x) = n(x)$. Plugging in the above for $h(x)$ lends us

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

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

Canceling $h(x)$ from both sides leads us to

$$0 = m(x)\frac{g(x)f(x)}{d(x)} - n(x)\frac{f(x)g(x)}{d(x)}$$

Dividing by $\frac{g(x)f(x)}{d(x)}$ and adding $n(x)$ to both sides yields

$$m(x) = n(x)$$

To show that any choice of $m(x)$ works, set $m(x)$ to some arbitrary polynomial and write the equation

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

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

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

The right side goes to zero and the left side is by definition $h(x)$. Hence, any choice of $m(x)$ will work.

Therefore, for particular solutions $a_0(x), b_0(x)$, the full set of solutions is

$$a(x) = a_0(x) + m(x)\frac{g(x)}{d(x)}$$

$$b(x) = b_0(x) - m(x)\frac{f(x)}{d(x)}$$

as $m(x)$ varies over $\mathbb{Q}[x]$. □

Problem 2.12. Let $F[x, y_1, y_2, ...]$ be the polynomial ring in the infinite set of variables $x, y_1, y_2, ...$ over the field F, and let I be the ideal $(x - y_1^2, y_1 - y_2^2, ..., y_i - y_{i+1}^2, ...)$ in the ring. Define R to be the ring $F[x, y_1, y_2, ...]/I$, so that in R the square of each y_{i+1} is y_i and $y_1^2 = x$ modulo I, ie. x has the $2i$ 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 $R_1 \subseteq R_2 \subseteq ...$ and that R is the union of all R_n ie. $R = \bigcup_{n=1}^{\infty} R_n$.

(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.

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

Proof. **(a)** First, note that $F \subseteq R_n$ for all n. So to complete the proof, we only need to show that for any natural number n, R_n contains $x, x^{1/2}, ..., x^{1/2^n}$. We are given that R_n contains $x^{1/2^n}$. Thus, it also contains $(x^{1/2^n})^2 = x^{1/2^{n-1}}$. This implies that R_n contains R_{n-1} as a subset. By induction, $R_1 \subseteq R_2 \subseteq ....$ □

Proof. **(b)** Define the function $\phi_n : R_n \to F[x]$ as $\phi_n(r(x)) = r(x^{2^n})$ for any $r(x) \in R_n$. This function amounts to bijective a relabeling of variables and is hence an isomorphism.

Furthermore, we are left with only whole numbered powers. To see this, note that every non whole numbered power in $r(x)$ has the form $x^{1/2^m}$ where $m \leq n$. The function sends this variable to $(x^{2^n})^{1/2^m} = x^{2^{n-m}}$.

Hence, $\phi_n(r(x))$ will be a polynomial with only positive whole numbered powers over F. Stated another way, R_n is isomorphic to a polynomial ring on one variable over F. Therefore, R_n is a PID.

To prove that R is a Bezout domain, take any two nontrivial principle ideals in R, $(x^1/2^n), (x^1/2^m)$. These ideals are contained in $R_{\max(m,n)}$. Since $R_{\max(m,n)}$ is a PID, $(x^1/2^n), (x^1/2^m)$ is principle in $R_{\max(m,n)}$. But an ideal that is principle on a subring containing itself is also principle on the entire ring. Therefore, $(x^1/2^n), (x^1/2^m)$ is principle on R. Hence, R is a Bezout domain. □

Proof. **(c)** Suppose for the sake of contradiction that $(x, x^{1/2}, x^{1/4}, ...)$ has finite generators. Let $1/2^n$ be the minimal degree of the polynomials in the set. Then, $(x, x^{1/2}, x^{1/4}, ...)$ is contained entirely in R_n. But R_n does not contain the element $x^1/2^{n+1}$ which is one of the generators of our ideal, which is a contradiction. Hence, $(x, x^{1/2}, x^{1/4}, ...)$ does not have finite generators. □

Problem 3.1. Let R be an integral domain with quotient field F and let $p(x)$ be a monic polynomial in $R[x]$. Assume that $p(x) = a(x)b(x)$ where $a(x)$ and $b(x)$ are monic polynomials in $F[x]$ of smaller degree than $p(x)$. Prove that if $a(x) \notin R[x]$ then R is not a unique factorization domain. Deduce that $\mathbb{Z}[2\sqrt{2}]$ is not a UFD.

Proof. (I am assuming by "quotient field" they mean "field of fractions." I believe this is a typo.)

First, note that the product of monic polynomials will be a monic polynomial. So, $p(x)$ must be a monic polynomial.

Corollary 6 states that if R is a UFD with fraction field F then a monic polynomial $p(x) \in R[x]$ is reducible in $R[x]$ if and only if it is reducible in $F[x]$. Suppose R is a UFD, then $p(x)$ must be reducible in

$R[x]$. So, there must be $a'(x)$, $b'(x)$ in $R[x]$ such that $a'(x)b'(x) = p(x)$. However, $F[x]$ is a UFD (Corollary 4). Being elements of $F[x]$ as well as $R[x]$, $a'(x)$ and $b'(x)$ would represent a different factorization of $p(x)$ than the one given. This is a contradiction; hence, $R[x]$ is not a UFD, and by Theorem 7, neither is R.

To prove the second part, Consider the polynomial $x^2 + 2\sqrt{2}x + 2$ in $\mathbb{Z}[2\sqrt{2}, x]$. This polynomial can be factored into monic parts $(x + \sqrt{2})^2$ which are only in $\mathbb{Q}[2\sqrt{2}, x]$. By the above, $\mathbb{Z}[2\sqrt{2}]$ is not a UFD. □

Problem 3.3. Let F be a field. Prove that the set R of polynomials in $F[x]$ whose coefficient of x is equal to 0 is a subring of $F[x]$ and that R is not a UFD. [Show that $x^6 = (x^2)^3 = (x^3)^2$ gives two distinct factorizations of x^6 into irreducibles.]

Proof. The set R is the same as the set of polynomials of the form $r(x) = a + x^2p(x)$ where a is some element of F and $p(x)$ is some polynomial in $F[x]$. This set is closed on addition and multiplication for if $r_1 = a + x^2p(x), r_2 = b + x^2q(x)$ are in R, then

$$r_1 + r_2 = a + x^2p(x) + b + x^2q(x) = (a + b) + x^2(p(x) + q(x)) \in R$$

$$r_1 \cdot r_2 = (a + x^2p(x)) \cdot (b + x^2q(x)) = ab + x^2(aq(x) + bp(x) + x^2p(x)q(x)) \in R$$

□

Hence, it is a subring.

To show it is a UFD, consider the element x^6. The polynomials x^2 and x^3 are both irreducible in R. Since $x^6 = (x^3)(x^3) = (x^2)(x^2)(x^2)$, x^6 has two distinct factorizations in R. Thus, R is a not a UFD.

Problem 3.5. Let $R = \mathbb{Z} + x\mathbb{Q}[x] \subset \mathbb{Q}[x]$ be the ring considered in the previous exercise. (that is, the set of polynomials in x with rational coefficients whose constant term is an integer.)

(a) Suppose that $f(x), g(x) \in \mathbb{Q}[x]$ are two nonzero polynomials with rational coefficients and that x^r is the largest power of x dividing both $f(x)$ and $g(x)$ in $\mathbb{Q}[x]$, (i.e. r is the degree of the lowest order term appearing in either $f(x)$ or $g(x)$). Let f_r and g_r be the coefficients of x^r in $f(x)$ and $g(x)$ respectively (one of wich is nonzero by definition of r). Then $\mathbb{Z}f_r + \mathbb{Z}g_r = \mathbb{Z}d_r$ for some nonzero $d_r \in \mathbb{Q}$Prove that there is a polynomial $d(x) \in \mathbb{Q}[x]$ that is a gcd of $f(x)$ and $g(x)$ in $\mathbb{Q}[x]$ and whose term of minimal degree is d_rx^r.

(b) Prove that $f(x) = d(x)q_1(x)$ and $g(x) = d(x)q_2(x)$ where $q_1(x)$ and $q_2(x)$ are elements of the subring R of $\mathbb{Q}[x]$.

Proof. **(a)** Let $d(x)$ be a gcd of $f(x)$ and $g(x)$ in $\mathbb{Q}[x]$. We have that $f(x) + g(x) = d(x)a(x)$ for some $a(x)$ in $\mathbb{Q}[x]$. Since x^r divides both $f(x)$ and $g(x)$, it must also divide their gcd $d(x)$. Since x^{r+1} does not divide the left side of the equation, and x^r does divide $d(x)$, x does not divide $a(x)$. Therefore, $a(x)$ has a nonzero constant term a_r and the minimal degree term in $d(x)$ is d_rx^r.

The minimal degree term on both sides is x^r, so we can divide out by x^r rendering $\frac{f(x)}{x^r} + \frac{g(x)}{x^r} = a(x) \cdot \frac{d(x)}{x^r}$. The constant terms in the equation will be $f_r + g_r = a_rd_r$. □

Problem 4.1. Determine whether the following polynomials are irreducible in the rings indicated. For those that are reducible, determine their factorization into irreducibles. The notation $\mathbb{F}_p$ denotes the finite field $\mathbb{Z}/p\mathbb{Z}$, p a prime.

(a) $x^2 + x + 1$ in $\mathbb{F}_2[x]$.

(b) $x^3 + x + 1$ in $\mathbb{F}_3[x]$.

(c) $x^4 + 1$ in $\mathbb{F}_5[x]$.

(d) $x^4 + 10x^2 + 1$ in $\mathbb{Z}[x]$.

Proof. **(a)** The field $\mathbb{F}_2$ contains only the elements 0 and 1. Plugging these values into the first polynomial we see $0^2+0+1 = 1$ and $1^2+1+1 = 3$, so neither element is a root. By proposition 9 and 10, the polynomial is not reducible. □

(b). The field $\mathbb{F}_3$ consists of the integers 0, 1, and 2. Plugging 1 in to the equation $1^3 + 1 + 1 = 0$, we see it is a root. So the polynomial $x - 1$ is a factor. In $\mathbb{F}_3$, $x - 1$ is $x + 2$. By proposition 9 and 10, there must be a polynomial $p(x)$ such that $(x + 2)p(x) = x^3 + x + 1$. By polynomial long division, which I am too lazy to write up here in latex, we have $p(x) = x^2 + x + 2$ Hence, $x^3 + x + 1 = (x + 2)(x^2 + x + 2)$ □

(c). The field $\mathbb{F}_5[x]$ holds the set of integers 0 ,1, 2, 3, and 4. Plugging each of these into the polynomial yields 1, 2, 17, 82, and 257 none of which are conguent to 0 mod(5). So, the polynomial has no factors of degree 1. But, since the polynomial is of degree 4, proposition 10 does not apply.

To factor the polynomial, note that $1 \cong -4 mod(5)$. So, the polynomial can be rewritten as $x^4 - 4 = (x^2)^2 - 2^2 = (x^2 + 2)(x^2 - 2) = (x^2 + 2)(x^2 + 3)$. As discussed earlier, the polynomial has no degree one roots. So, it is fully reduced. □

(d). By proposition 11, if the polynomial has a root, it must be a rational number whose numerator divides 1 and denominator also divides 1. That is to say, the root must be 1, if it exists. Plugging 1 in however yields $1^4 + 10 \cdot 1^2 + 1 = 12$. So, the polynomial has no degree one roots.

Both factors must then be degree 2. The form of the polynomial suggests that if it does factor, it has the form $(ax^2 + b)(cx^2 + d)$ where $ac = 1$, $bd = 1$, and $ad + bc = 10$. There are no units in the integers other than 1 and -1. So, we must have $a = b = c = d = 1$, $a = b = c = d = -1$, $a = c = -b = -d1$ or $-a = -c = b = d = 1$. But for all options $ab + cd \neq 10$, so there is no such factorization. □

Problem 4.3. Show that the polynomial $(x - 1)(x - 2)...(x - n) - 1$ is irreducible over $\mathbb{Z}$ for all $n \geq 1$.

Proof. Suppose the polynomial does factor into $p(x)q(x)$. Then if $x = 1, 2, ...n$, $p(x)q(x) = -1$ implying that $p(x) = 1$ and $q(x) = -1$ or $p(x) = -1$ and $q(x) = 1$ for each such x.

The polynomial $p(x) + q(x)$ has degree less than n. But, $x = 1, 2, ...n$ are all roots of this polynomial. Which is a contradiction. Therefore, there is no such factorization. □

Problem 4.5. Find all monic irreducible polynomials of degree ≤ 3 in $\mathbb{F}_2[x]$ and the same in $\mathbb{F}_3[x]$.

Proof. Such polynomials will have the form $ax^3 + bx^2 + cx + d.$ with 16 and 27 total options for $\mathbb{F}_2[x]$ and $\mathbb{F}_3[x]$ respectively. We will ignore polynomials with a constant term of 0, because they reduce to $xp(x)$. So our possible number goes down to 8 and 18.

By proposition 10, the irreducible polynomials are those without roots in their coefficient fields.

So, the irreducible polynomials in $\mathbb{F}_2$ are those with an odd number of coefficients ie. $1, x^2+x+1, x^3+x+1$, and $x^3 + x^2 + 1$.

We can use simple trial and error to find the polynomials in $\mathbb{F}_3[x]$. The irreducible polynomials where each coefficient is the same will are those polynomials whose number of terms do not divide 3 ie. $x + 1, 2x + 2, x^2 + 1, 2x^2 + 2, x^3 + 1, 2x^3 + 2, x^3 + x^2 + x + 1$, and $2x^3 + 2x^2 + 2x + 2$.

□

Problem 4.7. Prove that $\mathbb{R}[x]/(x^2 + 1)$ is a field isomorphic to the complex numbers.

Proof. First, since $x^2 + 1 = (x + i)(x - i)$, it is not reducible in $\mathbb{R}$. Hence, $\mathbb{R}/(x^2 + 1)$ is a field.

Next, notice that $x^2 + 1 \cong 0 \text{mod}(x^2 + 1)$ so $x^2 \cong -1 \text{mod}(x^2 + 1)$. So, any power of x greater than one can be reduced with $x^{2n} \cong (-1)^n$ and $x^{2n+1} = (-1)^n x$. Thus, every polynomial in $\mathbb{R}/(x^2 + 1)$ will have the form $a + bx$.

Define a function $\phi : \mathbb{R}[x]/(x^2 + 1) \to \mathbb{C}$ as $\phi(a + bx) = a + bi$. We want to show that this function is a ring homomorphism. Let $a + bx$ and $c + dx$ be two polynomials in our field. For addition,

$$\phi(a + bx) + \phi(c + dx) = a + bi + c + di = (a + c) + (b + d)i = \phi((a + c) + (b + d)i) = \phi(a + bx + c + dx)$$

And, on multiplication we have

$$\phi(a + bx) \cdot \phi(c + dx) = (a + bi) \cdot (c + di) = ac - bd + (ad + bc)i = \phi(ac - bd + (ad + bc)x) = \phi((a + bx) \cdot (c + dx))$$

Therefore, ϕ is a homomorphism. The kernel of ϕ is clearly 0, and so it is also an isomorphism. Thus, the two fields are isomorphic. □

Problem 4.9. Prove that the polynomial $x^2 - \sqrt{2}$ is irreducible over $\mathbb{Z}[\sqrt{2}]$ (you may use the fact that $\mathbb{Z}[\sqrt{2}]$ is a UFD — cf. Exercise 9 of Section 8.1).

Proof. The prime ideal $(\sqrt{2})$ in $\mathbb{Z}[\sqrt{2}]$ contains $\sqrt{2}$. But $(\sqrt{2})^2 = (2)$ does not contain $\sqrt{2}$. Hence, by Eisenstein's Criterion, the polynomial is irreducible. □

Problem 4.11. Prove that $x^2 + y^2 - 1$ is irreducible in $\mathbb{Q}[x, y]$.

Proof. Consider the prime ideal $(y^2 - x)$. Taking the mod of the given polynomial over this ideal yields $x^2 + x - 1$ which is not reducible in $\mathbb{Q}[x, y]$.

The polynomials in $\mathbb{Q}[x, y]$ which become units in $\mathbb{Q}[x, y]/(y^2 - x)$ are those whose constant term is in (1) and whose non-constant terms are divisible by $(y^2 - x)$. Such a term cannot factor out of $x^2 + y^2 - 1$. Therefore, by proposition 12, $x^2 + y^2 - 1$ is irreducible in $\mathbb{Q}[x, y]$. □

Problem 4.13. Prove that $x^3 + nx + 2$ is is irreducible over $\mathbb{Z}$ for all integers $n \neq 1, -3, -5$.

Proof. By proposition 10, this polynomial factors over $\mathbb{Q}$ if and only if it has a root in $\mathbb{Q}$. Proposition 11 states that the rational roots of the polynomial must be -1, -2, 2 or 1.

Setting $x = 1, -1, 2, -2$, we can solve for n,

$$1^3 + n + 2 = 0, n = -3$$

$$(-1)^3 - n + 2 = 0, n = 1$$

$$2^3 + 2n + 2 = 0, n = -5$$

$$(-2)^3 - 2n + 2 = 0, n = -3$$

So the polynomial will only reduce in $\mathbb{Q}$ if n is equal to $-3, 1$ or -5. By extension, the polynomial will only reduce in $\mathbb{Z}$ if n is equal to $-3, 1$ or -5 □

Problem 4.15. Prove that if F is a field then the polynomial $X^n - x$ which has coefficients in the ring $F[[x]]$ of formal power series is irreducible over $F[[x]]$.

Proof. I am assuming that X is the variable and x is a constant. In other words, that the polynomial is in $F[[x]][X]$.

The ideal (x) is prime in $F[[x]]$. The polynomial $X^n - x$ is monic, with the constant term x being in the prime ideal (x), but not in the ideal $(x)^2$. Therefore, by Eisenstein's criterion, the polynomial is irreducible in $F[[x]]$. □

Problem 4.17. Prove the following variant of Eisenstein's Criterion: let P be a prime ideal in the Unique Factorization Domain R and let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ + a_1 x + a_0$ be a polynomial in $R[x]$, $n \geq 1$. Suppose $a_n \notin P$, $a_{n-1}, ..., a_0 \in P$ and $a_o \notin P^2$. Prove that $f(x)$ is irreducible in $F[x]$, where F is the quotient field of R.

Proof. Suppose the polynomial is reducible in $R[x]$. Then, $a_n x^n + a_{n-1}x^{n-1} + \ + a_1 x + a_0 = a(x)b(x)$. Note that $a(x)$ and $b(x)$ have nonzero constant terms. Also note that $a(x)$ and $b(x)$ have non zero max degree terms $a'_k x^k$ and $b_m x^m$ where $k + m = n$, and $a'_k, b_m \notin P$.

Taking the modulus of both sides by P, we have $a_n x^n = \overline{a(x)b(x)}$, using the convention that bars denote passage from R to R/P. Since a_0 is in P and not in P^2, then without loss of generality, $a(x)$ must have a constant term $a'_0 \notin P$. But then, $\overline{a(x)b(x)}$ would have the term $a'_0 b_m x^m$, a contradiction. Hence, $f(x)$ is not reducible in R. By Gauss' Lemma, it is also irreducible in F.

(It is odd that my proof for proposition 13 works for non $a_n \neq 1$, yet doesn't require R to be a UFD. The textbook author assume $a_n = 1$ when they did the proof fo any integral domains, but this doesn't seem necessary.) □

Problem 4.19. Let F be a field and let $f(x) = a_n x^n + a_{n-1}x^{n-1} + . + a_o \in F[x]$. The derivative, $D_x(f(x))$, of $f(x)$ is defined by

$$D_x(f(x)) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ + a_1$$

where, as usual, $na = a + a + \ + a$ (n times). Note that $D_x(f(x))$ is again a polynomial with coefficients in F.

The polynomial $f(x)$ is said to have a multiple root if there is some field E containing F and some $\alpha \in E$ such that $(x-\alpha)^2$ divides $f(x)$ in $E[x]$. For example, the polynomial $f(x) = (x-1)^2(x-2) \in \mathbb{Q}[x]$ has $\alpha = 1$ as a multiple root and the polynomial $f(x) = x^4 + 2x^2 + 1 = (x^2+1)^2 \in \mathbb{R}[x]$ has $\alpha = \pm i \in \mathbb{C}$ as multiple roots. We shall prove in Section 13.5 that a nonconstant polynomial $f(x)$ has a multiple root if and only if $f(x)$ is not relatively prime to its derivative (which can be detected by the Euclidean Algorithm in $F[x]$). Use this criterion to determine whether the following polynomials have multiple roots:

(a) $x^3 - 3x - 2 \in \mathbb{Q}[x]$

(b) $x^3 + 3x + 2 \in \mathbb{Q}[x]$

(c) $x^6 - 4x^4 + 6x^3 + 4x^2 - 12x + 9 \in \mathbb{Q}[x]$

(d) Show for any prime p and any $a \in \mathbb{F}_p$ that the polynomial $x^p - a$ has a multiple root.

Proof. **(a)** The derivative of the polynomial is $3x^2 - 3$, which has factorization $3(x-1)(x+1)$. -1 is a root of the original polynomial, so it must share the factor $(x+1)$ with its derivative. Hence, they are not relatively prime and $x^3 - 3x - 2$ has multiple roots. □

(b). The derivative of the polynomial is $3x^2 + 3$, which does not factor in $\mathbb{Q}[x]$. So, if the polynomials are not relatively prime, there must be a polynomial $ax + b$ such that $x^3 + 3x + 2 = (3x^2 + 3)(ax + b)$. But then $b \cdot 3 = 2$ and $b \cdot 3 = 0$, which is impossible in $\mathbb{Q}[x]$. So, the polynomials are relatively prime and $x^3 + 3x + 2$ does nt have multiple roots. □

(c). The derivative of this polynomial is $6x^5 - 16x^3 + 18x^2 + 8x - 12$. We can use polynomial long division and the Euclidean algorithm or Wolfram Alpha to find the gcd. I'll let you guess which one I did, but the polynomials have gcd 1. Hence, they are relatively prime and $x^6 - 4x^4 + 6x^3 + 4x^2 - 12x + 9$ therefore does not contain multiple roots. □

(d). The derivative of this polynomial will be px^{p-1}, which is 0 in $\mathbb{F}_p[x]$, which is obviously divisible by $x^p - a$. Hence, $x^p - a$ is not relatively prime to its derivative and it has multiple roots. □

Problem 5.1. Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Describe the nilradical of $F[x]/(f(x))$ in terms of the factorization of $f(x)$ (cf. Exercise 29, Section 7.3).

Proof. The nilradical of $F[x]/(f(x))$ are those elements which are the root of elements in $(f(x))$. (ie. a is in the niradical if $a^n \in (f(x))$ for some n). If $f(x)$ has distinct prime factorization $f_1(x)^{m_1} f_2^{m_2}(x)...f_k^{m_k}(x)$, then the nonzero elements of the nilradical will be $l = f_1(x)^{n_1} f_2^{n_2}(x)...f_k^{n_k}(x)$, where $n_i > 0$ and at least one $n_i < m_i$. The first stipulation is necessary for and guaranties that $l^j \in (f(x))$ for some j, because this is a UFD and each $f_i(x)$ is prime. The second stipulation ensures that l is not already in $(f(x))$. □

Problem 5.3. Let p be an odd prime in $\mathbb{Z}$ and let n be a positive integer. Prove that $x^n - p$ is irreducible over $\mathbb{Z}[i]$. [Use Proposition 18 in Chapter 8 and Eisenstein's Criterion.]

Proof. We want to find an ideal P such that $p \in P$ but $p \notin P^2$. The ring $\mathbb{Z}[i]$ is principle and hence is a UFD. So an equivalent task is finding a prime q in $\mathbb{Z}[i]$ such that $q|p$ but $q^2 \not| p$. To do this, we consider the possible factors of p.

(I am ashamed to say I cheated on this one with math overflow. I wasn't sure how proposition 18 applied here. So, I looked it up to find the following lemma) If $p = 3 mod 4$, then it is prime in $\mathbb{Z}[i]$. So, $p \in (p)$ but $p \notin (p^2)$. If $p = 1 mod 4$, then it is the product $(a+bi)(a-bi)$ where both factors are prime. In that case, $p \in (a+bi)$ but $p \notin (a+bi)^2$.

Either way, there is an ideal containing p whose square does not contain p. Hence, by Eisenstein's criterion, $x^n - p$ is irreducible in $\mathbb{Z}[i]$. □

Problem 5.5. Let ϕ denote Euler's ϕ-function. Prove the identity $\Sigma_{d|n}\phi(d) = n$, where the sum is extended over all the divisors d of n. [First observe that the identity is valid when $n = p^m$ is the power of a prime p since the sum telescopes. Write $n = p^m n'$ where p does not divide n'. Prove that $\Sigma_{d|n}\phi(d) = \Sigma_{d''|p^m}\phi(d'')\Sigma_{d'|n'}\phi(d')$ by multiplying out the right hand side and using the multiplicity $\phi(ab) = \phi(a)\phi(b)$ when a and b are relatively prime. Use induction to complete the proof. This problem may be done alternatively by letting Z be the cyclic group of order n and showing that since Z contains a unique subgroup of order d for each d dividing n, the number of elements of Z of order d is $\phi(d)$. Then $|Z|$ is the sum of $\phi(d)$ as d runs over all divisors of n.]

Proof. (First method) The only numbers that divide p^m are $1, p, p^2, ..., p^m$. So, we can rewrite the sum as $\Sigma_{n\leq m}\phi(p^n) = (1) + (p-1) + (p^2-p) + (p^3-p^2) + ... + (p^m - p^{m-1})$ which telescopes to p^m. We are given that $\phi(ab) = \phi(a)\phi(b)$ when a and b are relatively prime. So, if $n = p^m n'$, where n' does not divide p^m, then

$$\Sigma_{d|n}\phi(d) = \Sigma_{d'|n', d''|p^m}\phi(d'd'') = \Sigma_{d'|n', d''|p^m}\phi(d')\phi(d'')$$

Which can be factored into the sums

$$= \Sigma_{d''|p^m}\phi(d'')\Sigma_{d'|n'}\phi(d') = p^m\Sigma_{d''|n}\phi(d'')$$

There are two cases for n'. Either $n' = 1$, in which case we are done. Or, by the fundamental theorem of arithmetic, n' is the product of prime powers and we can continmue the algorithm until $n' = 1$. So, by induction, the theorem is true.

(Second method) Let Z be the cyclic sub group of order n, $(\mathbb{Z}/n\mathbb{Z})^x$. By corollary 20, part 1, $(\mathbb{Z}/n\mathbb{Z})^x = (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^x \text{x} ... \text{x} (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^x$ where $p_1, ..., p_r$ are primes such that $n = p_1^{\alpha_1}...p_r^{\alpha_r}$. Hence, Z has a subgroup of order $p_i^{\alpha_i}$ for each of n's r prime divisors. □

Problem 5.7. Prove that the additive and multiplicative groups of a field are never isomorphic. [Consider three cases: when $|F|$ is finite, when $-1 \neq 1$ in F, and when $-1 = 1$ in F.]

Proof. If $|F|$ is finite, then the multiplicative group must be cyclical. Suppose there is an isomorphism ϕ from the multiplicative group to the additive one. Then, the additive group of the ring must be cyclical as well. □

Problem 6.1. Suppose I is an ideal in $F[x_1, ..., x_n]$ generated by a (possibly infinite) set $\mathcal{S}$ of polynomials. Prove that a finite subset of the polynomials in $\mathcal{S}$ suffice to generate I . [Use Theorem 21 to write $I = (f_1, ..., f_m)$ and then write each $f_i \in I$ using polynomials in $\mathcal{S}$.]

Proof. Corollary 22 states that $F[x_1, ..., x_n]$ is finitely generated. So there are polynomials $f_0, ..., f_n$ such that $I = (f_0, ..., f_m)$. We can write each f_i in terms of elements of $\mathcal{S}$, lending a generator of I in terms of a finite subset of $\mathcal{S}$. Hence, that finite subset of $\mathcal{S}$ generates I. □

Problem 6.3. Prove that if $\geq$ is any total or partial ordering on a nonempty set then the following are equivalent:

- **(i)** Every nonempty subset contains a minimum element
- **(ii)** There is no infinite strictly decreasing sequence $a_1 > a_2 > a_3 > ...$ (This is called a descending chain condition or DCC)

Deduce that general polynomial division always terminates in finitely many steps.

Proof. Every set $(a_1, a_2, ...)$ will have a least element if and only if there is some $a_i \in (a_1, a_2, ...)$ such that there is no $a_j \in (a_1, a_2, ...)/a_i$ where $a_i > a_j$. This is true if and only if there is no infinite strictly decreasing sequence $a_1 > a_2 > a_3 > ...$, since such a sequence would necessarily terminate with the sets minimal element.

Each step in general polynomial long division ensures that the leading term of the dividend, on the given lexicographic ordering, is reduced. Hence, repeated application will tend towards a polynomial of leading term degree 0. □

Problem 6.5. The grevlex monomial ordering is defined by first choosing an ordering of the variables $x_1, x_2, ..., x_n$. then defining $m_1 \geq m_2$ for monomials m_1, m_2 if either $\deg m_1 > \deg m_2$ or $\deg m_1 = \deg m_2$ and the first exponent of $x_n, x_{n-1}, ..., x_1$ (in that order) where m_1 and m_2 differ is smaller in m_1.

(a) Prove that grevlex is a monomial ordering that satisfies $x_1 > x_2 > ... > x_n$.

(b) Prove that the grevlex ordering on $F[x_1, x_2]$ with respect to x_1, x_2 is the graded lexicographic ordering with $x_1 > x_2$, but that the grevlex ordering on $F[x_1, x_2, x_3]$ is not the grading of any lexicographic ordering.

(c) Show that $x_1x_2^2x_3 > x_1^2x_3^2 > x2xj > XtX2 > xi > XtX3 > xj' > x1 > x2$ for the grevlex monomial ordering with respect to x_1, x_2, x_3.

Proof. (a) For x_i, x_{i+1}, we can rewrite each as $x_i^1x_{i+1}^0$ and $x_i^0x_{i+1}^1$. Comparing these two terms, it is clear that $x_i > x_{i+1}$ for any i. □

(b). Any two monomials in $R[x_1, x_2]$ will have multidegrees (a, b) and (c, d). Their possible relationship states relevant to grevlex are a subset of $\{e_d, n\}X\{l_1, g_1, e_1\}X\{l_2, g_2, e_2\}$. The first symbol indicates whether the degrees are equal, the second indicates the ordered relation between a and c, and the third indicates the ordered relation between b and d. For example, if $a = c$ and $d < b$, we have their relation as (n, e_1, l_2), which gets sorted into $m_1 < m_2$ on grevlex.

Given two monomials m_1, m_2 in such a relational state, their relation on grevlex can be sorted as

$$m_1 = m_2 : (e, e_1, e_2), (e, l_1, g_2), (e, g_1, l_2)$$

$$m_1 < m_2 : (n, e_1,$$

This is a lot of writing on a problem that isn't super interesting. So, I'm gonna skip the rest for now and maybe forever. Sorry to whoever was enthralled by this stuff. □

Problem 6.7. Order the monomials $x^2z, x^2y^2z, xy^2z, x^3y, x^3z^2, x^2, x^2yz^2, x^2z^2$ for the lexicographic monomial ordering $x > y > z$, for the corresponding grlex monomial order, and for the grevlex monomial ordering with respect to $\{x, y, z\}$.

Proof. The lexicographic ordering is

$$x^3y > x^3z > x^2y^2z > x^2yz^2 > x^2z^2 > x^2z > x > xy^2z$$

The grlex monomial ordering is

$$x^2y^2z > x^2yz^2 > x^3y > x^3z > x^2z^2 > xy^2z > x^2z > x$$

Finally, the grevlex ordering is

$$x^2yz^2 > x^2y^2z > xy^2z > x^2z^2 > x^3z > x^3y > x^2z > x$$

□

(I am doing an even numbered exercise because problem 9 was another question on monomial ordering and I didn't feel like it was as good a use of my time)

Problem 6.10. Suppose I is a monomial ideal generated by monomials $m_1, ..., m_k$. Prove that the polynomial $f \in F[x_1, ...X_n]$ is in I if and only if every monomial term f_i of f is a multiple of one of the m_i. [For polynomials $a_1, ..., a_k \in F[x_1, ..., x_n]$ expand the polynomial $a_1m_1 + ... + a_km_k$ and note that every monomial term is a multiple of at least one of the m_1.] Show that $x^2yz + 3xy^2$ is an element of the ideal $J = (xyz, y^2) \subset F[x, y, z]$ but is not an element of the ideal $I' = (xz^2, y^2)$.

Proof. Let f be any element of I. Then, f is the product of some collection of polynomials $f_1, ..., f_k$ and the monomials generating I. So, we have $f = a_1m_1 + ... + a_km_k$. The monomials of f will be the sum of all $a_{i,j}m_i$ where $a_{i,j}$ is a monomial in f_i and the sum of the multidegrees of $a_{i,j}$ and m_i are equal. With some relabeling, we can write this as $\Sigma a_i m_1 + \Sigma a_i m_2 + ... + \Sigma a_i m_k$. Since the degree of the total sum must be less than the degree of each of the m_j, we can divide out my any m_j by multiplying the entire term by m_j^{-1},

$$m_j(\Sigma a_i m_1 m_j^{-1} + \Sigma a_i m_2 m_j^{-1} + ... + \Sigma a_i m_k m_j^{-1})$$

Thus, each monomial term in f is divisible by some m_j.

We can lable the generators of I as $m_1 = xyz, m_2 = y^2$. It is easy to see that $x^2yz + 3xy^2 = x(xyz) + 3x(y^2) = xm_1 + 3xm_2$. By the above theorem, $x^2yz + 3xy^2$ is an element of I. However, because the term x^yz is not a multiple of any monomial generator of $I' = (xz^2, y^2)$, it is not in I'. □

Problem 6.11. Fix a monomial ordering on $R = F[x_1, ..., x_n]$ and suppose $\{g_1, ..., g_m\}$ is a Gröbner basis for the ideal I in R. Prove that $h \in LT(I)$ if and only if h is a sum of monomial terms each divisible by some $LT(g_i)$, $1 \leq i \leq m$. [Use the previous exercise.]

Proof. By definition, the leading terms of the Gröbner basis are a basis for the the set of leading terms in I. So, h is in $LT(I)$ if and only if h is in $(LT(g_1), ..., LT(g_m))$. Since $h, LT(g_1), ..., LT(g_m)$ are all monomials, the previous exercise allows us to conclude that h is in $(LT(g_1), ..., LT(g_m))$ if and only if h is the sum of monomial terms each divisible by some $LT(g_i)$. □

Problem 6.13. Suppose I i s a monomial ideal with monomial generators $g_1, ..., g_m$. Use Buchberger's Criterion to prove that $\{g_1, ..., g_m\}$ is a Gröbner basis for I.

Proof. Buchberger's Criterion states that $\{g_1, ..., g_m\}$ is a Gröbner basis for I if an only if $S(g_i, g_j) \cong 0 \mathrm{mod} I$ for all $i \neq j$. We wish to show this for the given basis. Since $g_1, ..., g_m$ are monomials, $LT(g_i) = g_i$ for all i. The function $S(g_i, g_j)$ hence becomes

$$S(g_i, g_j) = \frac{M}{LT(g_i)}g_i - \frac{M}{LT(g_j)}g_j = \frac{M}{g_i}g_i - \frac{M}{g_j}g_j = M - M = 0$$

Hence, Buchberger's Criterion holds and $\{g_1, ..., g_m\}$ is therefore a Gröbner basis. □

Problem 6.15. Fix a monomial ordering on $R = F[x_1, ..., x_n]$.

(a) Prove that $\{g_1, ..., g_m\}$ is a minimal Gröbner basis for the ideal I in R if and only if $\{LT(g_1), ..., LT(g_m)\}$ is a minimal generating set for $LT(I)$.

(b) Prove that the leading terms of a minimal Gröbner basis for I are uniquely determined and the number of elements in any two minimal Gröbner bases for I is the same. [Use (a) and the previous exercise.]

Proof. (a) By definition, a Gröbner basis is minimal if each leading term is monic and no term g_j is divisible by any $LT(g_i)$ for $i \neq j$.

Suppose $\{g_1, ..., g_m\}$ is a minimal Groöbner basis. Further suppose for the sake of contradiction that $(LT(g_1), ..., LT(g_m))$ is not minimal, say $LT(g_1)|LT(g_2)$. Then we can remove g_1 from $\{g_1, ..., g_m\}$ and the smaller basis $\{g_2, ..., g_m\}$ would still be, by definition, a Gröbner basis, which is a contradiction. Hence, if $\{g_1, ..., g_m\}$ is minimal then so is $(LT(g_1), ..., LT(g_m))$.

Now suppose $(LT(g_1), ..., LT(g_m))$ is minimal. Then, $LT(g_j)$ is not divisble by any $LT(g_i)$. Thus, g_j is also not divisible by any $LT(g_j)$. Therefore, if $(LT(g_1), ..., LT(g_m))$ is minimal then so is $\{g_1, ..., g_m\}$. □

(b). By exercise 14, the generating set $(LT(g_1), ..., LT(g_m))$ is unique. Hence, the leading terms in the minimal Gröbner basis $\{g_1, ..., g_m\}$ are uniquely determined. Since $\{g_1, ..., g_m\}$ is only minimal if $(LT(g_1), ..., LT(g_m))$ is minimal, any Gröbner basis for I must have m terms. □

Problem 6.17. Fix the lexicographic ordering $x > y$ on $F[x, y]$. Use Buchberger's Criterion to show that $x^2y - y^2, x^3 - xy$ is a Gröbner basis for the ideal $I = (x^2y - y^2, x^3 - xy)$.

Proof. We only need to show that $S(x^2y - y^2, x^3 - xy) = 0$.

The lcm of the leading terms is x^3y. Plugging this into the formula yields

$$S(x^2y - y^2, x^3 - xy) = x(x^2y - y^2) - y(x^3 - xy) = x^3y - xy^2 - x^3y - xy^2 = 0$$

Thus, by Buchberger's Criterion, $x^2y - y^2, x^3 - xy$ is a Gröbner basis.

□

Problem 6.19. Fix the lexicographic ordering $x > y$ on $F[x, y]$.

(a) Show that $\{x^3 - y, x^2y - y^2, xy^2 - y^2, y^3 - y^2\}$ is the reduced Gröbner basis for the ideal $I = (-x^3 + y, x^2y - y^2)$.

(b) Determine whether the polynomial $f = x^6 - x^5y$ is an element of the ideal I.

Proof. (a) We will show this by first proving that $\{x^3 - y, x^2y - y^2, xy^2 - y^2, y^3 - y^2\}$ is a gröbner basis for I, using Buchberger's Criterion. Then, we show that it is fully reduced.

For easier notation, we label the elements of $\{x^3 - y, x^2y - y^2, xy^2 - y^2, y^3 - y^2\}$ as g_1 to g_4 respective of their given order. We also label the ideal they generate as J Now we compute $S(g_i, g_j)$ for each $g_i \neq g_j$.

$$S(g_1, g_2) = y(x^3 - y) - x(x^2y - y^2) = x^3y - y^2 - x^3y + xy^2 = xy^2 - y^2 = -x(x^2y - y^2) + y(x^3 - y) - xg_2 + yg_1 \in J$$

$$S(g_1, g_3) = y^2(x^3 - y) - x^2(xy^2 - y^2) = x^3y^2 - y^3 - x^3y^2 + x^2y^2 = y(x^2y - y^2) = y(g_2) \in J$$

$$S(g_1, g_4) = y^3(x^3 - y) - x^3(y^3 - y^2) = x^3y^3 - y^4 - x^3y^3 + x^3y^2 = -y^2(x^3 - y^2) = y^2(g_1) \in J$$

$$S(g_2, g_3) = y(x^2y - y^2) - x(xy^2 - y^2) = x^2y^2 - y^3 - x^2y^2 + xy^2 = -y(-x^3 + y) - x(x^2y - y^2) = yg_1 - xg_2 \in J$$

$$S(g_2, g_4) = y^2(x^2y - y^2) - x^2(y^3 - y^2) = x^2y^3 - y^4 - x^2y^3 + x^2y^2 = y(x^2y - y^2) - y(y^3 - y^2) = yg_2 - yg_4 \in J$$

$$S(g_3, g_4) = y(xy^2 - y^2) - x(y^3 - y^2) = xy^3 - y^3 - xy^3 + xy^2 = (xy^2 - y^2) - (y^3 - y^2) \in J$$

Hence, $\{x^3 - y, x^2y - y^2, xy^2 - y^2, y^3 - y^2\}$ is a Gröbner basis. To see that it is fully reduced, note that no leading term divides any other leading term and every leading term is monic.

Now, we need to show that it is a basis for I. We again for ease of notation will denote the generators of I as f_1 and f_2. First note that $f_1 = -g_1$ and $f_2 = g_2$. So, I is a generated by J. We also have that $g_1 = -f_1$, $g_2 = f_2$, $g_3 = -yf_1 - xf_2$, and $g_4 = yf_2 - (x - 1)(-yf_1 - xf_2)$. Thus, I generates G. The ideals generate each other, so they must be the same ideal.

Therefore, $\{x^3 - y, x^2y - y^2, xy^2 - y^2, y^3 - y^2\}$ is the minimal Gröbner basis for I. □

(b). By theorem 23.2, we can use general polynomial division. Let $f = x^6 - x^5y$ and as before, the elements of the Gröbner basis are $g_1, ..., g_4$. The leading term x^6 is divisible by $LT(g_1)$. So we iterate to $q_1 = x^3$ and $f = -x^5y + yx^3$. The leading term is again divisible by $LT(g_1)$. So, we iterate to $q_1 = x^3 - x^2y$ and $f = yx^3 - y^2x^2$. The leading term is divisible by $LT(g_2)$. So we iterate to $q_2 = x$ and $f = -y^2x^2 + xy^2$. This leading term is divisible by $LT(g_3)$, so we iterate to $q_3 = -x$ and $f = 0$.

The algorithm terminated with no remainder. By Theorem 23.3, $x^6 - x^5y$ is in I. □

Problem 6.21. Fix the lexicographic ordering $x > y$ on $F[x, y]$. Use Buchberger's Criterion to show that $\{x^2y - y^2, x^3 - xy\}$ is a Gröbner basis for the ideal $I = (x^2y - y^2, x^3 - xy)$.

Proof. The lcm of the leading terms is x^3y. Applying the S function to the polynomials gives

$$S(x^2y - y^2, x^3 - xy) = \frac{x^3y}{x^2y}(x^2y - y^2) - \frac{x^3y}{x^3}(x^3 - xy) = x(x^2y - y^2) - y(x^3 - xy) = x^3y - xy^2 - x^3y + xy^2 = 0$$

Since 0 is trivially in I, we have that $\{x^2y - y^2, x^3 - xy\}$ is a Gröbner basis for I. □

Problem 6.23. Show that the ideals $I = (x^2y + xy^2 - 2y, x^2 + xy - x + y^2 - 2y, xy^2 - x - y + y^3)$ and $J = (x - y^2, xy - y, x^2 - y)$ in $F[x, y]$ are equal.

Proof. Label the polynomials in the generator of I as f_1 to f_3 and the polynomials in J's generator as g_1 to g_3

By corollary 28, I and J are the same if and only if they have the same reduced Gröbner basis.

We can use Buchberger's algorithm to find these bases. We begin with the first ideal. $S(f_1, f_2) = (x^2y + xy^2 - 2y) - y(x^2 + xy - x + y^2 - 2y) = x^2y + xy^2 - 2y - x^2y - xy^2 + xy - y^3 - 2y^2 = xy - y^3 - 2y^2 - 2y$ □

Problem 6.25. Show that the reduced Gröbner basis using the lexicographic ordering $x > y$ for the ideal $I = (x^2 + xy^2, x^2 - y^3, y^3 - y^2)$ is $\{x^2 - y^2, y^3 - y^2, xy^2 + y^2\}$.