

# Exercises from Chapter 9

Wesley Basener

May 24, 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  $x_1, x_2, \dots, x_n$  are independent variables over  $R$ , prove that  $R[x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)}]$  is isomorphic to  $R[x_1, x_2, \dots, x_n]$  for any permutation of  $\{1, 2, \dots, n\}$ .

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

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

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

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

$$\phi((\sum_{i_1=0}^m (\sum_{i_2=0}^m \dots (\sum_{i_n=0}^m \alpha_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}) \dots))) + \phi((\sum_{i_1=0}^m (\sum_{i_2=0}^m \dots (\sum_{i_n=0}^m \beta_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}) \dots))) =$$

$$\phi((\sum_{i_1=0}^m (\sum_{i_2=0}^m \dots (\sum_{i_n=0}^m \alpha_{i_1, i_2, \dots, i_n} x_{\pi(1)}^{i_1} x_{\pi(2)}^{i_2} \dots x_{\pi(n)}^{i_n}) \dots))) + \phi((\sum_{i_1=0}^m (\sum_{i_2=0}^m \dots (\sum_{i_n=0}^m \beta_{i_1, i_2, \dots, i_n} x_{\pi(1)}^{i_1} x_{\pi(2)}^{i_2} \dots x_{\pi(n)}^{i_n}) \dots))) =$$

$$\phi((\sum_{i_1=0}^m (\sum_{i_2=0}^m \dots (\sum_{i_n=0}^m (\alpha_{i_1, i_2, \dots, i_n} + \beta_{i_1, i_2, \dots, i_n}) x_{\pi(1)}^{i_1} x_{\pi(2)}^{i_2} \dots x_{\pi(n)}^{i_n}) \dots))) =$$

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

Hence, the function satisfies the homomorphism condition on addition.

For multiplication, the coefficient of the term  $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$  in  $\phi(\alpha \cdot \beta)$  will be the sum of all  $\alpha_{k_1, k_2, \dots, k_n} \cdot \beta_{j_1, j_2, \dots, j_n}$  where  $k_1 + j_1 = i_{\pi^{-1}(1)}, k_2 + j_2 = i_{\pi^{-1}(2)}, \dots, k_n + j_n = i_{\pi^{-1}(n)}$  are all true. The coefficients of the  $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$  term in  $\phi(\alpha) \cdot \phi(\beta)$  will be the sum of all  $\alpha_{k_1, k_2, \dots, k_n} \cdot \beta_{j_1, j_2, \dots, j_n}$  where  $k_{\pi(1)} + j_{\pi(1)} = i_1, k_{\pi(2)} + j_{\pi(2)} = i_2, \dots, k_{\pi(n)} + j_{\pi(n)} = i_n$  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  $R[x_1, x_2, \dots, x_n]$  are the set of units in  $R$ , and  $\phi$  is the identity element on  $R$ ,  $\phi(1_{R[x_1, x_2, \dots, x_n]}) = 1_{R[x_1, x_2, \dots, x_n]}$ .

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

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

**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  $\alpha = \sum_{i=0, j=0}^{m, n} \alpha_{i, j} x^i y^j$  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.  $\square$

**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  $\mathbb{Q}[x, y]$ .  $\square$

**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.  $\square$

**Problem 1.8.** Let  $F$  be a field and  $R = F[x, x^2y, x^3y^2, \dots, x^ny^{n-1}, \dots]$  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  $x$ . Therefore, the fraction field is  $(F, x, y) = F[x, y]$ .

For part b, consider the ideal of elements  $fx^my^n$ , 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  $a_2, b_2$  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.  $\square$

**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  $R[x_1, x_2, \dots]$ , 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.  $\square$

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

*Proof.* Consider the ideal  $(x_{\beta_1}, x_{\beta_2}, \dots)$ , where  $\beta_1$  is either  $1$  or  $2$ ,  $\beta_2$  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  $(x_1x_2, x_3x_4, x_5x_6, \dots)$ . 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  $\beta$ s, there are infinite such minimal ideals in the ring.  $\square$

**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.  $\square$

**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  $\bar{P} = (\bar{x}, \bar{y})$  is a prime ideal. Show that  $\overline{xy} \in \bar{P}^2$  but that no power (This shows that  $\bar{P}$  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  $\overline{P}^2$ .  $\square$

**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  $\phi : B \rightarrow A$ . 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  $\phi((y - x) \cdot (y + x)) = \phi(y - x) \cdot \phi(y + x)$  is also in the kernel of  $A$ .

But since  $\phi$  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  $F$ .  $\square$

**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  $\phi$  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  $\phi$  is the ideal  $(x^i - y^j)$ . To see this, notice that

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

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

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

$\square$

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

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

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

Since the exponents sum to  $k$ , we have

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

$\square$

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

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

$$\begin{aligned} (\sum_{i=0}^k a_i x_1^{e_{i,1}} x_2^{e_{i,2}} \dots x_n^{e_{i,n}}) \cdot (\sum_{i=0}^m b_i x_1^{l_{i,1}} x_2^{l_{i,2}} \dots x_n^{l_{i,n}}) &= \sum_{i=0}^k \sum_{j=0}^m (a_i x_1^{e_{i,1}} x_2^{e_{i,2}} \dots x_n^{e_{i,n}}) \cdot (b_j x_1^{l_{j,1}} x_2^{l_{j,2}} \dots x_n^{l_{j,n}}) \\ &= \sum_{i=0}^k \sum_{j=0}^m (a_i x_1^{e_{i,1}} x_2^{e_{i,2}} \dots x_n^{e_{i,n}}) \cdot (b_j x_1^{l_{j,1}} x_2^{l_{j,2}} \dots x_n^{l_{j,n}}) = \sum_{i=0}^k \sum_{j=0}^m a_i b_j x_1^{e_{i,1}+l_{j,1}} x_2^{e_{i,2}+l_{j,2}} \dots x_n^{e_{i,n}+l_{j,n}} \end{aligned}$$

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

**Problem 1.17.** An ideal  $I$  in  $R[x_1, \dots, x_n]$  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  $R[x_1, \dots, x_n]$ . 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  $p \cdot \sum_{i=0}^n a_i x_1^{e_{i,1}} x_2^{e_{i,2}} \dots x_n^{e_{i,n}}$  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  $\sum_{i=0}^n p \cdot a_i x_1^{e_{i,1}} x_2^{e_{i,2}} \dots x_n^{e_{i,n}}$ . The polynomial is now the sum of of the terms  $p \cdot a_i x_1^{e_{i,1}} x_2^{e_{i,2}} \dots x_n^{e_{i,n}}$ , each of which have the desired property.  $\square$

**Problem 1.18.** Let  $R$  be an arbitrary ring and let  $\text{Func}(R)$  be the ring of all functions from  $R$  to itself. If  $p(x) \in R[x]$  is a polynomial, let  $f_p \in \text{Func}(R)$  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  $\overline{1}, \overline{x}, \dots, \overline{x^{n-1}}$  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.  $\square$

**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  $q^n$ .  $\square$

**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 if  $f(x)$  is irreducible, which of course is true if and only if  $F[x]/(f(x))$  is a field.  $\square$

**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  $p_0(x), p_1(x), \dots, p_n(x)$ . Consider the product of all these polynomials plus one,  $p_0(x) \cdot p_1(x) \cdot \dots \cdot p_n(x) + 1$ . 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.  $\square$

**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  $(\bar{1})$  and  $(\bar{0})$ . From corollary 4,  $F[x]/(p(x))$  is a PID, so any ideal will have a single generator. Suppose  $\bar{q(x)}$  is a generator for a non trivial ideal in  $F[x]/(p(x))$ , if one exists. We can rewrite  $(\bar{q(x)})$  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  $p(x) = p_0(x) \cdot p_1(x) \cdot \dots \cdot p_n(x)$ , 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  $[0, n]$ .  $\square$

**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.  $\square$

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

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

We can rewrite the above as

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

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

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

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

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

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

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  $F[x, y_1, y_2, \dots]$  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 the 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  $I$ , 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  $R_1 \subseteq R_2 \subseteq \dots$  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  $x, x^{1/2}, x^{1/4}, \dots$  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  $x, x^{1/2}, \dots, x^{1/2^n}$ . 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,  $R_1 \subseteq R_2 \subseteq \dots$  □

*Proof.* (b) Define the function  $\phi_n : R_n \rightarrow F[x]$  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  $(x, x^{1/2}, x^{1/4}, \dots)$  has finite generators. Let  $1/2^n$  be the minimal degree of the polynomials in the set. Then,  $(x, x^{1/2}, x^{1/4}, \dots)$  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,  $(x, x^{1/2}, x^{1/4}, \dots)$  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  $\mathbb{Z}[\sqrt{2}]$  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.  $\square$

**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

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

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

$\square$

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 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 which 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  $d_r x^r$ .

(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  $f(x) = d(x)a(x)$  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  $d_r x^r$ .

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  $f_r + g_r = a_r d_r$ .  $\square$

**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.  $\square$

(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,  $x^3 + x + 1 = (x + 2)(x^2 + x + 2)$   $\square$

(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 congruent 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  $1 \cong -4 \text{ mod}(5)$ . 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.  $\square$

(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  $a = b = c = d = 1$ ,  $a = b = c = d = -1$ ,  $a = c = -b = -d = 1$  or  $-a = -c = b = d = 1$ . But for all options  $ab + cd \neq 10$ , so there is no such factorization.  $\square$

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

*Proof.* Suppose the polynomial does factor into  $p(x)q(x)$ . Then if  $x = 1, 2, \dots, n$ ,  $p(x)q(x) = -1$  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,  $x = 1, 2, \dots, n$  are all roots of this polynomial. Which is a contradiction. Therefore, there is no such factorization.  $\square$

**Problem 4.5.** Find all monic irreducible polynomials of degree  $\leq 3$  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 be 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  $2x^3 + 2x^2 + 2x + 2$ .  $\square$

**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  $x^{2n+1} \cong (-1)^n x$ . Thus, every polynomial in  $\mathbb{R}/(x^2 + 1)$  will have the form  $a + bx$ .

Define a function  $\phi : \mathbb{R}[x]/(x^2 + 1) \rightarrow \mathbb{C}$  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,

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

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,  $\phi$  is a homomorphism. The kernel of  $\phi$  is clearly 0, and so it is also an isomorphism. Thus, the two fields are isomorphic.  $\square$

**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.  $\square$

**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  $\mathbb{Q}[x, y]$ .  $\square$

**Problem 4.13.** Prove that  $x^3 + nx + 2$  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  $-5$ .  $\square$

**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  $F[[x]]$ .  $\square$

**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  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  be a polynomial in  $R[x]$ ,  $n \geq 1$ . Suppose  $a_n \notin P$ ,  $a_{n-1}, \dots, a_0 \in P$  and  $a_0 \notin P^2$ . 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,  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = a(x)b(x)$ . 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 for any integral domains, but this doesn't seem necessary.)  $\square$

**Problem 19.** Let  $F$  be a field and let  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in F[x]$ . The derivative,  $D_x(f(x))$ , of  $f(x)$  is defined by

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

where, as usual,  $na = a + a + \dots + a$  ( $n$  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.  $\square$

(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 not have multiple roots.  $\square$

(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.  $\square$

(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.  $\square$