

4.2.5a Use the Euclidean Algorithm to find the gcd of the given polynomials:

$$x^4 - x^3 - x^2 + 1 \quad \text{and} \quad x^3 - 1 \quad \text{in} \quad \mathbb{Q}[x]$$

Applying the Euclidean Algorithm we obtain,

$$\begin{aligned} x^4 - x^3 - x^2 + 1 &= (x^3 - 1)(x - 1) + (-x^2 + x) \\ x^3 - 1 &= (-x^2 + x)(-x - 1) + (x - 1) \\ -x^2 + x &= (x - 1)(-x) + 0. \end{aligned}$$

Hence the the last nonzero remainder,  $x - 1$  is a common divisor of highest degree and, since it is monic, it is the gcd of the two polynomials.  $\blacklozenge$

4.2.8 Let  $f(x), g(x) \in F[x]$ , not both zero, and let  $d(x)$  be their gcd. If  $h(x)$  is a common divisor of  $f(x)$  and  $g(x)$  of highest possible degree then prove that  $h(x) = cd(x)$  for some nonzero  $c \in F$ .

Let  $h(x)$  be a common divisor of  $f(x)$  and  $g(x)$  of highest possible degree. By definition of the gcd,  $d(x)$  is itself a common divisor of  $f(x)$  and  $g(x)$  of highest degree. Hence,  $\deg h(x) = \deg d(x)$ . Moreover, by Corollary 4.6,  $h(x) \mid d(x)$ . So  $d(x) = h(x)k(x)$  for some polynomial  $k(x)$ . But since  $F$  is a field and therefore an integral domain we have (by Theorem 4.2)

$$\deg d(x) = \deg h(x) + \deg k(x) = \deg d(x) + \deg k(x);$$

hence,  $\deg k(x) = 0$  and so  $k(x) = k$  for some nonzero constant  $k \in F$ . Thus,  $h(x) = cd(x)$ , where  $c = k^{-1} \in F$  (note that  $c$  is nonzero).  $\blacklozenge$

4.3.5 Prove that  $f(x)$  and  $g(x)$  are associates in  $F[x]$  if and only if  $f(x) \mid g(x)$  and  $g(x) \mid f(x)$ .

Note that we must assume that the  $f(x)$  and  $g(x)$  are nonzero polynomials in order for the problem to make sense. Recall that the units in  $F[x]$  are precisely the nonzero elements of  $F$  (see Corollary 4.9). So two nonzero polynomials are associates if and only if one is a nonzero constant multiple of the other. Suppose first that  $f(x)$  and  $g(x)$  are associates in  $F[x]$ . Then  $f(x) = cg(x)$  for some nonzero  $c \in F$ . Hence,  $f(x) \mid g(x)$  and, since,  $g(x) = c^{-1}f(x)$ , we also have  $g(x) \mid f(x)$ .

Conversely, suppose that  $f(x) \mid g(x)$  and  $g(x) \mid f(x)$ . It follows that

$$\deg f(x) \leq \deg g(x) \leq \deg f(x) \quad \text{and hence} \quad \deg f(x) = \deg g(x).$$

But since  $f(x) \mid g(x)$  we have  $f(x) = g(x)h(x)$  for some  $h(x) \in F[x]$ . By Theorem 4.2,

$$\deg f(x) = \deg g(x) + \deg h(x).$$

But since  $\deg f(x) = \deg g(x)$ ,  $\deg h(x) = 0$  and  $h(x) = c$  for some nonzero  $c \in F$ . Thus,  $f(x) = cg(x)$  and so  $f(x)$  and  $g(x)$  are associates.  $\blacklozenge$

4.3.23 a. Show that  $x^2 + 2$  is irreducible in  $\mathbb{Z}_5[x]$ .

Suppose to the contrary that  $x^2 + 2$  is reducible. Then  $x^2 + 2 = (x + a)(x + b)$  for some  $a, b \in \mathbb{Z}_5$ . Hence,

$$x^2 + 2 = (x + a)(x + b) = x^2 + (a + b)x + ab.$$

It follows that  $a + b = 0$  and  $ab = 2$ , that is,  $b = -a$  and  $a^2 = -ab = -2 = 3$ . It is easy to check that for any element  $a \in \mathbb{Z}_5$ ,  $a^2 = 0, 1$  or  $4$ . This contradicts the requirement that  $a^2 = 3$ . Hence,  $x^2 + 2$  is irreducible in  $\mathbb{Z}_5[x]$ . It is even easier to show that  $x^2 + 2$  is irreducible in  $\mathbb{Z}_5[x]$  using the methods of 4.4. One checks that for all  $a \in \mathbb{Z}_5$ ,  $a^2 + 2 \neq 0$ . Hence,  $x^2 + 2$  has no roots and is therefore irreducible by Corollary 4.18.  $\blacklozenge$

b. Factor  $x^4 - 4$  as a product of irreducibles in  $\mathbb{Z}_5[x]$ .

From part (a) we know that  $x^2 + 2$  is irreducible in  $\mathbb{Z}_5[x]$  and a similar argument shows that  $x^2 + 3$  is irreducible. Hence, the desired factorization is  $x^4 - 4 = (x^2 + 2)(x^2 + 3)$ .  $\blacklozenge$

4.4.4 a. For what value of  $k$  is  $x - 2$  a factor of  $x^4 - 5x^3 + 5x^2 + 3x + k$  in  $\mathbb{Q}[x]$ ?

Set  $f(x) = x^4 - 5x^3 + 5x^2 + 3x + k$ . We apply the Factor Theorem which states that  $x - 2$  is a factor of  $f(x)$  in  $\mathbb{Q}[x]$  if and only if 2 is a root of  $f(x)$ , that is,

$$0 = f(2) = 2^4 - 5 \cdot 2^3 + 5 \cdot 2^2 + 3 \cdot 2 + k = k + 2.$$

So  $x - 2$  a factor of  $x^4 - 5x^3 + 5x^2 + 3x + k$  in  $\mathbb{Q}[x]$  if  $k = -2$ .  $\blacklozenge$

b. For what value of  $k$  is  $x + 1$  a factor of  $x^4 + 2x^3 - 3x^2 + kx + 1$  in  $\mathbb{Z}_5[x]$ ?

Set  $f(x) = x^4 + 2x^3 - 3x^2 + kx + 1$ . We apply the Factor Theorem which states that  $x + 1 = x - 4$  is a factor of  $f(x)$  in  $\mathbb{Z}_5[x]$  if and only if 4 is a root of  $f(x)$ , that is,

$$0 = f(4) = 4^4 + 2 \cdot 4^3 - 3 \cdot 4^2 + k \cdot 4 + 1 = 4k + 2.$$

So  $x + 1$  a factor of  $x^4 + 2x^3 - 3x^2 + kx + 1$  in  $\mathbb{Z}_5[x]$  if  $4k + 2 = 0$  or  $k = 2$ .  $\blacklozenge$

4.4.17 Find a polynomial of degree 2 in  $\mathbb{Z}_6[x]$  that has four roots in  $\mathbb{Z}_6$ . Does this contradict Corollary 4.16?

Observe that  $a^2 = a$  for  $a = 0, 1, 3, 4 \in \mathbb{Z}_6$ . Hence,  $x^2 - x = x^2 + 5x$  has four roots in  $\mathbb{Z}_6[x]$ . This does not contradict Corollary 4.16 because  $\mathbb{Z}_6$  is not a field and so the Corollary does not apply.  $\blacklozenge$