4.2 Factors

from A Study Guide for Beginner’s by J.A.Beachy,
a supplement to Abstract Algebra by Beachy / Blair

This section introduces concepts for polynomials that model those for integers. The division algorithm for polynomials is similar to that of integers, except that the remainder is determined by its degree (which replaces the size of an integer). We can define the greatest common divisor of two polynomials, and we can find it via the Euclidean algorithm. This, in turn, leads to a unique factorization theorem, in which the notion of an irreducible polynomial replaces that of a prime number.

In Chapter 1 we used a matrix method to write \( \gcd(a, b) \) as a linear combination of \( a \) and \( b \). A similar result holds for polynomials, but in solving the corresponding problems for polynomials use the “back-substitution” method. Trying to put polynomials into a matrix just gets too complicated.

SOLVED PROBLEMS: §4.2

21. Over the field of rational numbers, use the Euclidean algorithm to show that \( 2x^3 - 2x^2 - 3x + 1 \) and \( 2x^2 - x - 2 \) are relatively prime.
   Let \( 2x^3 - 2x^2 - 3x + 1 = f(x) \) and \( 2x^2 - x - 2 = g(x) \).

22. Over the field of rational numbers, find the greatest common divisor of \( x^3 - 1 \) and \( x^4 + x^3 + 2x^2 + x + 1 \), and express it as a linear combination of the given polynomials.

23. Find the greatest common divisor of \( x^3 - 2x + 1 \) and \( x^2 - x - 2 \) in \( \mathbb{Z}_5[x] \), and express it as a linear combination of the given polynomials.

24. (a) Express \( x^4 + x \) as a product of polynomials irreducible over \( \mathbb{Z}_5 \).
   (b) Show that \( x^3 + 2x^2 + 3 \) is irreducible over \( \mathbb{Z}_5 \). 

25. Express \( 2x^3 + x^2 + 2x + 2 \) as a product of polynomials irreducible over \( \mathbb{Z}_5 \).

26. Factor \( x^4 + 2 \) over \( \mathbb{Z}_3 \).

27. Factor \( x^4 + 1 \) over \( \mathbb{Z}_2 \), over \( \mathbb{Z}_5 \), over \( \mathbb{Z}_7 \), and over \( \mathbb{Z}_{11} \).

28. Find a polynomial \( q(x) \) such that \( (a + bx)q(x) \equiv 1 \pmod{x^2 + 1} \) over \( \mathbb{Z}_3 \).

29. Let \( F \) be a field, and let \( f(x), g(x) \in F[x] \), with \( \deg(f(x)) = n \) and \( \deg(g(x)) = m \), where \( m < n \in \mathbb{Z}^+ \). Write \( n = qm + r \), where \( r = 0 \) or \( r < m \). Show that there exist polynomials \( r_0(x), r_1(x), \ldots, r_q(x) \) such \( f(x) = r_q(x)g(x)^q + \ldots + r_1(x)g(x) + r_0(x) \), where \( \deg(r_i(x)) < m \) for \( 0 \leq i \leq q \).

30. Let \( F \) be a field, and let \( f(x) \in F[x] \). Prove that \( f(x) \) is irreducible over \( F \) if and only if \( f(x + c) \) is irreducible over \( F \).
MORE PROBLEMS: §4.2

31. Show that \( x^4 - 4x^3 + 4x^2 + 17 \) has no repeated roots in \( \mathbb{Q} \).

32. Show that \( x^4 + 4x^2 - 4x - 3 \) has no repeated roots in \( \mathbb{Q} \).

33.† Over \( \mathbb{Z}_3 \), find \( \text{gcd}(x^5 - x^4 + x^3 - x^2, x^3 - x^2 + x - 1) \) and write it as a linear combination of the given polynomials.

34.† Over \( \mathbb{Z}_5 \), find \( \text{gcd}(x^5 + x^4 - 2x^3 - x^2 + 2x - 2, x^3 - x^2 + x - 1) \) and write it as a linear combination of the given polynomials.

35.† Over \( \mathbb{Z}_7 \), find \( \text{gcd}(x^5 + 3x^4 - 2x^3 - 3x - 3, x^3 - x^2 + x - 1) \) and write it as a linear combination of the given polynomials.

36.† Over \( \mathbb{Q} \), find \( \text{gcd}(x^5 - 8x^4 + 25x^3 - 38x^2 + 28x - 8, x^5 - x^4 - 2x^3 + 2x^2 + x - 1) \) and write it as a linear combination of the given polynomials.

37. Factor \( x^4 + 2 \) over \( \mathbb{Z}_3 \)

38. Factor \( x^4 + x^3 + x^2 + 1 \) over \( \mathbb{Z}_2 \).

39.† Factor \( x^3 + 6 \) over \( \mathbb{Z}_7 \).

40.† Show that \( x^4 + 1 \) has a proper factorization over \( \mathbb{Z}_p \), for all primes \( p \).