4.1 Fields; Roots of Polynomials

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

25. Let $F$ be a field, and let $f(x), g(x) \in F[x]$ be polynomials of degree less than $n$. Assume that $f(x)$ agrees with $g(x)$ on $n$ distinct elements of $F$. (That is, $f(x_i) = g(x_i)$ for distinct elements $x_1, \ldots, x_n \in F$.) Prove that $f(x) = g(x)$ (as polynomials).

Solution: Look at the polynomial $p(x) = f(x) - g(x)$. It is either zero or has degree less than $n$. The given condition shows that $p(x)$ has $n$ distinct roots in $F$, given by $x_1, \ldots, x_n$. This contradicts Corollary 4.1.12 unless $p(x) = 0$ is the zero polynomial, and so we must have $f(x) = g(x)$.

26. Let $c \in F$ and let $f(x) \in F[x]$. Show that $r \in F$ is a root of $f(x)$ if and only if $r - c$ is a root of $f(x + c)$.

Solution: Let $g(x) = f(x + c)$ be the polynomial we get after making the substitution of $x + c$ in place of $x$. If $r$ is a root of $f(x)$, then $f(r) = 0$, and so substituting $r - c$ into $g(x)$ gives us $g(r - c) = f(r - c + c) = f(r) = 0$. Conversely, if $r - c$ is a root of $g(x)$, then $g(r - c) = 0$, so $f(r) = f(r - c + c) = g(r - c) = 0$ and $r$ is a root of $f(x)$.

27. For $f(x) = x^3 - 5x^2 - 6x + 2 \in \mathbb{Q}[x]$, use the method of Theorem 4.1.9 to write $f(x) = q(x)(x + 1) + f(-1)$.

Solution: We have $f(-1) = -1 - 5 + 6 + 2 = 2$. Therefore
\[
f(x) - f(-1) = (x^3 - (-1)^3) - 5(x^2 - (-1)^2) - 6(x - (-1)) + (2 - 2) = (x + 1)((x^2 - x + 1) - 5(x - 1) - 6) = (x + 1)(x^2 - 6x),
\]
and so $f(x) = (x^2 - 6x)(x + 1) + 2$.

28. For $f(x) = x^3 - 2x^2 + x + 3 \in \mathbb{Z}_7[x]$, use the method of Theorem 4.1.9 to write $f(x) = q(x)(x - 2) + f(2)$.

Solution: For simplicity, we will just write $a$ for the elements of $\mathbb{Z}_7$, rather than $[a]_7$. We have $f(2) = 8 - 8 + 2 + 3 = 5$. Therefore
\[
f(x) - f(2) = (x^3 - (2)^3) - 2(x^2 - (2)^2) + (x - 2) + (3 - 3) = (x - 2)((x^2 + 2x + 4) - 2(x + 2) + 1) = (x - 2)(x^2 + 1),
\]
and so $f(x) = (x^2 + 1)(x - 2) + 5$.

29. Show that the set of matrices of the form $\begin{bmatrix} a & b \\ -3b & a \end{bmatrix}$, where $a, b \in \mathbb{Q}$, is a field under the operations of matrix addition and multiplication.

Solution: Since a linear algebra course is a prerequisite for this text, it is fair to assume that the associative and distributive laws hold for matrix addition and multiplication. It is also true that addition is commutative, though multiplication need not
satisfy the commutative law. To check that we have a field, it is sufficient to check
the closure properties, the existence of identities and inverses, and commutativity of
multiplication.

(i) Closure of + and ·:
\[
\begin{bmatrix}
  a & b \\
-3b & a
\end{bmatrix} + \begin{bmatrix}
  c & d \\
-3d & c
\end{bmatrix} = \begin{bmatrix}
  (a + c) & (b + d) \\
-3(b + d) & (a + c)
\end{bmatrix} \in F
\]
\[
\begin{bmatrix}
  a & b \\
-3b & a
\end{bmatrix} \begin{bmatrix}
  c & d \\
-3d & c
\end{bmatrix} = \begin{bmatrix}
  (ac - 3bd) & (ad + bc) \\
-3(ad + bc) & (ac - 3bd)
\end{bmatrix} \in F
\]

(iii) In the given set, multiplication is commutative:
\[
\begin{bmatrix}
  a & b \\
-3b & a
\end{bmatrix} \begin{bmatrix}
  c & d \\
-3d & c
\end{bmatrix} = \begin{bmatrix}
  ac - 3bd & ad + bc \\
-3(ad + bc) & ac - 3bd
\end{bmatrix} = \begin{bmatrix}
  c & d \\
-3d & c
\end{bmatrix} \begin{bmatrix}
  a & b \\
-3b & a
\end{bmatrix}.
\]

(v) Identity Elements: The matrices \[
\begin{bmatrix}
  0 & 0 \\
0 & 0
\end{bmatrix} \text{ and } \begin{bmatrix}
  1 & 0 \\
0 & 1
\end{bmatrix} \text{ belong to } F \text{ and are the identity elements.}
\]

(vi) Inverse Elements: The negative of \[
\begin{bmatrix}
  a & b \\
-3b & a
\end{bmatrix}
\]
is nonzero, then at least one of \(a\) or \(b\) is nonzero, so the determinant \(a^2 + 3b^2\) is nonzero since \(\sqrt{3}\) is not a rational number. The standard formula for the
inverse of a 2 \(\times\) 2 matrix yields \[
\begin{bmatrix}
  a & b \\
-3b & a
\end{bmatrix}^{-1} = \frac{1}{a^2 + 3b^2} \begin{bmatrix}
  a & -b \\
-3(-b) & a
\end{bmatrix} \in F.
\]

30. Prove that if \(p\) is a prime number, then the multiplicative group \(\mathbb{Z}_p^\times\) is cyclic.

Solution: We will use Proposition 3.5.9 (b), which states that a finite abelian group
is cyclic if and only if its exponent is equal to its order. Suppose that the exponent
of \(\mathbb{Z}_p^\times\) is \(m\). Then \(a^m = 1\) for all nonzero \(a \in \mathbb{Z}_p^\times\), and so the polynomial \(x^m - 1\) has
\(p - 1\) distinct roots in \(\mathbb{Z}_p^\times\). It follows from Corollary 4.1.12 that \(m = p - 1\), and so \(\mathbb{Z}_p^\times\)
must be cyclic.

31. Let \(p\) be a prime number, and let \(a, b \in \mathbb{Z}_p^\times\). Show that if neither \(a\) nor \(b\) is a square,
then \(ab\) is a square.

Solution: By Problem 30, we can choose a generator \(\alpha\) for \(\mathbb{Z}_p^\times\). If neither \(a\) nor \(b\) is a
square, then \(a = \alpha^s\) and \(b = \alpha^t\), where \(s\) and \(t\) are odd. Therefore \(ab = (\alpha^s)^2\), where
\(s + t = 2k\), and so \(ab\) is a square.

32. Use the method of divided differences to find the polynomial of degree 2 whose graph
passes through \((0, 5)\), \((1, 7)\), and \((-1, 9)\).
Solution: Let \( p(x) \) be the polynomial we are looking for. We get the following table of differences, where the entry in the 3rd column is \( \frac{-4}{3(-1)} \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>( p(n) )</th>
<th>( p(n) )</th>
<th>( p(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>5</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>-1</td>
<td>9</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This gives us the polynomial \( p(x) = 9 + (-4)(x - (-1)) + 3(x - (-1))(x - 0) = 9 - 4x - 4 + 3x^2 + 3x = 3x^2 - x + 5 \). Check: \( p(0) = 5, \ p(1) = 7, \ p(-1) = 9. \)

33. Use the method of divided differences to find a formula for \( \sum_{i=1}^{n} i^2. \)

Solution: We know that \( 1 + 2 + \cdots + n = n(n+1)/2. \) This suggests that the formula for the sum of squares might be a cubic polynomial in \( n. \) Let’s write \( p(n) = \sum_{i=0}^{n} i^2. \) Then \( p(0) = 0, \ p(1) = 0^2+1^2 = 1, \ p(2) = 0^2+1^2+2^2 = 5, \) and \( p(3) = 0^2+1^2+2^2+3^2 = 14. \)

We get the following table of differences.

<table>
<thead>
<tr>
<th>( n )</th>
<th>( p(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>14</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

This gives the polynomial \( p(n) = 0+1(n-0)+\frac{3}{2}(n-0)(n-1)+\frac{1}{3}(n-0)(n-1)(n-2) = n(1+\frac{3}{2}n-\frac{3}{2} + \frac{1}{3}n^2 - n + \frac{2}{3}) = \frac{1}{6}n(2n^2 + 3n + 1) \), which simplifies to the well-known formula \( p(n) = \frac{1}{6}n(n+1)(2n+1). \)

**ANSWERS AND HINTS**

34. Find the number of elements \( a \in \mathbb{Z}_p \) for which \( x^2 - a \) has a root in \( \mathbb{Z}_p. \)

Answer: \((p + 1)/2\)

39. Use the method of divided differences to find the cubic polynomial whose graph passes through the points \((0, -5), (1, -3), (-1, -11), \) and \((2, 1).\)

Answer: \( 1 + 4(x - 2) + 1(x - 2)(x - 1) + 1(x - 2)(x - 1)(x - 0) = -5 + 3x - 2x^2 + x^3 \)

41. Use the method of divided differences to verify the formula for \( \sum_{i=1}^{n} i^3. \)

Answer: \( n + \frac{3}{2}n(n-1) + 2n(n-1)(n-2) + \frac{1}{3}n(n-1)(n-2)(n-3) = \frac{1}{4}n^2(n+1)^2 \)

42. Let \( F \) be a finite field, and let \( f(x) : F \to F \) be any function. Prove that there exists a polynomial \( p(x) \in F[x] \) such that \( f(a) = p(a) \) for all \( a \in F. \)

Hint: Use the Lagrange interpolation formula.