Math 531 Homework 9

Theo Koss

April 2021

1 Section 4.3

- Problem 1: Let F be a field. Given $p(x) \in F[x]$, prove that congruence modulo $p(x)$ defines an equivalence relation on $F[x]$.

  Proof. We N2S 3 things,

  (1) Reflexivity: For any $f(x) \in F[x]$,

  $$f(x) - f(x) = 0 \equiv 0 \mod p(x)$$

  $$\implies f(x) \equiv f(x) \mod p(x)$$

  Therefore this relation is reflexive.

  (2) Symmetry: Let $f(x), g(x) \in F[x]$.
  Assume that $f(x) \equiv g(x) \mod p(x)$.

  $$\implies p(x)|f(x) - g(x)$$

  $$\implies p(x)| - [f(x) - g(x)]$$

  $$\implies p(x)|g(x) - f(x)$$

  $$g(x) = f(x) \mod p(x)$$

  Therefore congruence modulo $p(x)$ is symmetric.

(3) Transitivity: Let $f(x), g(x), h(x) \in F[x]$.
Assume that $f(x) \equiv g(x) \mod p(x)$ and $g(x) \equiv h(x) \mod p(x)$.

$$\implies p(x) | f(x) - g(x), \text{ and } p(x) | g(x) - h(x)$$
$$\implies p(x) | [f(x) - g(x)] + [g(x) - h(x)]$$
$$\implies p(x) | f(x) - h(x)$$
$$\implies f(x) \equiv h(x) \mod p(x)$$

Therefore congruence modulo $p(x)$ is transitive.

Since 1,2,3 are true, congruence modulo $p(x)$ is an equivalence relation.
QED

- Problem 3: Let E be a field, and F a subfield of E. Prove that the multiplicative identity of F must be the same as that of E.

Proof. Call the multiplicative identity of F, 1_F, and call that of E, 1_E.

$$1_E \cdot 1_F = 1_F$$

Since 1_F belongs to E, and F is a subfield of E. Also,

$$1_E \cdot 1_F = 1_E$$

Because 1_F is the identity of F, by definition, this is true. Therefore,

$$1_E \cdot 1_F = 1_F = 1_E$$

As required. QED

- Problem 11: Let F be any field. Prove that the field of $n \times n$ scalar matrices over F is isomorphic to F.

Proof. Let F be any field, then let F' be the field of $n \times n$ scalar matrices with inputs from F.

$$F' = \left\{ \begin{bmatrix} a & 0 & \dots & 0 \\ 0 & a & & \\ \vdots & & \ddots & \\ 0 & & & a \end{bmatrix} | a \in F \right\}$$

Define a map $\phi : F' \to F$.

$$\phi(a) = \phi(A) = \phi \begin{bmatrix} a & 0 & \dots & 0 \\ 0 & a & & \\ \vdots & & \ddots & \\ 0 & & & a \end{bmatrix} \longrightarrow a$$

N2S:

1. ϕ is a homomorphism:
   Let $A, B \in F'$, where $A = (a)$ and $B = (b)$. Then

   $$\phi(A+B) = \phi((a)+(b)) = a+b = \phi(a)+\phi(b) = \phi(A)+\phi(B)$$

   And

   $$\phi(AB) = \phi(ab) = ab = \phi(a)\phi(b) = \phi(A)\phi(B)$$

   Thus ϕ is a homomorphism.
2. ϕ is 1-1:
   Let

   $$\begin{aligned} &\phi(A) = \phi(B) \\ \implies &\phi(a) = \phi(b) \\ \implies &a = b \end{aligned}$$

   Since $A, B \in F'$, we can write them like so:

   $$A = \begin{bmatrix} a & 0 & \dots & 0 \\ 0 & a & & \\ \vdots & & \ddots & \\ 0 & & & a \end{bmatrix}, B = \begin{bmatrix} b & 0 & \dots & 0 \\ 0 & b & & \\ \vdots & & \ddots & \\ 0 & & & b \end{bmatrix}$$

   Since $a = b$ from above, this shows $A = B$. And thus $\phi(A) = \phi(B)$ implies $A = B$.
3. ϕ is onto: Let $a \in F$, then $A = \begin{bmatrix} a & 0 & \dots & 0 \\ 0 & a & & \\ \vdots & & \ddots & \\ 0 & & & a \end{bmatrix}$, and $\phi(A) = a$.
   Therefore $\forall a \in F$, $\exists A \in F'$ s.t. $\phi(A) = a$.

Now since $\phi : F' \to F$ is a homomorphism, 1-1 and onto, it is an isomorphism. QED

2 Section 4.4

- Problem 3: Find all integer roots of the following equations.

  (a) $x^3 + 8x^2 + 13x + 6 = 0$. $x = -1, -6$

  (b) $x^3 - 5x^2 - 2x + 24 = 0$. $x = -2, 3, 4$

  (c) $x^3 - 10x^2 + 27x - 18 = 0$. $x = 1, 3, 6$

  (d) $x^4 + 4x^3 + 8x + 32 = 0$. $x = -4, -2$

  (e) $x^7 + 2x^5 + 4x^4 - 8x^2 - 32 = 0$. No integer solutions.

- Problem 13: Verify each of the following, for complex numbers z and w.

  (a) $\overline{zw} = \overline{z} \cdot \overline{w}$
  Let $z = x + iy$, $w = u + iv$. Then

  $$zw = (x + iy)(u + iv) = xu - yv + i(xv + yu)$$

  $$\overline{zw} = (xu - yv) - i(xv + yu)$$

  And

  $$\overline{z} = x - iy, \overline{w} = u - iv$$

  $\overline{z} \cdot \overline{w} = (x - iy)(u - iv) = xu + i(xv + uy) - yv = (xu - yv) - i(xv + yu)$

  Thus $\overline{zw} = \overline{z} \cdot \overline{w}$.

  (b) $|zw| = |z||w|$
  Let $z = x + iy$, $w = u + iv$. Then

  $$zw = (x + iy)(u + iv) = (xu - yv) + i(xv + yu)$$

  $|zw| = \sqrt{(xu - yv)^2 + (xv + yu)^2} = \sqrt{x^2u^2 + y^2v^2 + x^2v^2 + y^2u^2}$

  and

  $$|z| = \sqrt{x^2 + y^2}, |w| = \sqrt{u^2 + v^2}$$

  $|z||w| = \sqrt{x^2 + y^2} \cdot \sqrt{u^2 + v^2} = \sqrt{(x^2 + y^2)(u^2 + v^2)} = \sqrt{x^2u^2 + y^2v^2 + x^2v^2 + y^2u^2}$

  Thus $|zw| = |z||w|$