

Homework 23 - MATH 791

Will Thomas

Problem 1:

Show that $p(x) = x^3 + x^2 + 2x + 1$ is irreducible over \mathbb{Z}_3 .

Solution:

Let us assume for contradiction that we could factor out some $(x - \alpha)$ for $\alpha \in \mathbb{Z}$.

Then we know that $x^3 + x^2 + 2x + 1 = (x - \alpha)(\beta_2x^2 + \beta_1x + \beta_0)$. Let us just destruct on possible values of α

$\alpha = 0$:

Then clearly this will not work as $(x)(\beta_2x^2 + \beta_1x + \beta_0)$ will have no constant term, but one is required.

$\alpha = 1$:

Then we will have $(x - 1)(\beta_2x^2 + \beta_1x + \beta_0)$ and the constant term will force $\beta_0 = -1 \equiv 2$.

We will also know that $\beta_2 = 1$ (from monic polynomial). This forces

$$\begin{aligned}(x - 1)(x^2 + \beta_1x + 2) &= x^3 + (2 + \beta_1x^2) + (-\beta_1x) + 1 \\ &= x^3 + x^2 + 2x + 1\end{aligned}$$

This equality is irreconcilable for any possible β_1

$\alpha = 2$:

Then we will have $(x - 2)(\beta_2x^2 + \beta_1x + \beta_0)$ and the constant term will force $\beta_0 = -2 \equiv 1$.

We will also know that $\beta_2 = 1$ (from monic polynomial). This forces

$$\begin{aligned}(x - 2)(x^2 + \beta_1x + 1) &= x^3 + (1 + \beta_1x^2) + (-2 * \beta_1x) + 1 \\ &= x^3 + x^2 + 2x + 1\end{aligned}$$

This equality is irreconcilable for any possible β_1

$\therefore p(x)$ is irreducible over \mathbb{Z}_3

Problem 2:

For $p(x)$ as in the previous problem, from class we know that there is a field K containing \mathbb{Z}_3 and $\alpha \in K$ such that $p(\alpha) = 0$.

(i) How many elements are in the field $\mathbb{Z}_3(\alpha)$?

(ii) In the field $\mathbb{Z}_3(\alpha)$ calculate $A \cdot B$ and A^{-1} for $A := 1 + 2\alpha + \alpha^2$ and $B := 2 + \alpha + 2\alpha^2$

Solution:

(i) We know that $p(x)$ is irreducible, and that its degree is 3

$$\therefore [\mathbb{Z}_3(\alpha) : \mathbb{Z}_3] = 3$$

We know that $\{0, 1, 2\} \in \mathbb{Z}_3$, and the basis for $\mathbb{Z}_3(\alpha)$ contains 1.

That means we have two extra elements in our basis and the closure of it would be the cross so $3^3 = 27$

Thus, there are 27 elements in $\mathbb{Z}_3(\alpha)$

(ii)

$$A \cdot B = 2 + 4\alpha + 2\alpha^2 + \alpha + 2\alpha^2 + \alpha^3 + 2\alpha^2 + 4\alpha^3 + 2\alpha^4$$

$$A \cdot B = 2 + 2\alpha + 2\alpha^3 + 2\alpha^4$$

$$A \cdot B = 2(1 + \alpha)(1 + \alpha^3)$$

As for A^{-1} , I do not want to calculate this.

Problem 3:

Give an example of a field with 125 elements.

Solution:

Admitted

Problem 4:

Fix a prime p . Assume that for all $n \geq 1$, there exists an irreducible polynomial in $\mathbb{Z}_p[x]$ having degree n . Show that for all primes p and $n \geq 1$, there exists a field with p^n elements.

Solution:

Admitted

Problem 5:

Let $\alpha \in K \supseteq \mathbb{Z}_2$ be a root of $x^2 + x + 1$. Show that $\mathbb{Z}_2(\alpha)$ is the splitting field for $x^2 + x + 1$.

Solution:

Admitted