Homework to chapters 33,46

Tuesday, November 19, 2019 8:31 PM

Let $\mathbb{F}_{p^n}$ denote the finite field with p^n elements. Recall that for any prime p and integer $n \geq 1$, $\mathbb{F}_{p^n}$ exists and is essentially unique.

① Show that $x^9 - x \in \mathbb{Z}_3[x]$ is a product of all irreducible monic polynomials of degree 1 and 2.

② Find all subfields of $\mathbb{F}_{64}$. How many $\alpha \in \mathbb{F}_{64}$ satisfy $\mathbb{F}_2(\alpha) = \mathbb{F}_{64}$

③ Consider the extension of finite fields $\mathbb{F}_4 \subset \mathbb{F}_{16}$. Show that for any $x \in \mathbb{F}_{16}$ we always have $x^5 \in \mathbb{F}_4$ (Hint: identify $\mathbb{F}_4 \subset \mathbb{F}_{16}$ as the subset of elements that satisfy $x^4 - x = 0$).

④ Consider the Euclidean Domain $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$ with the norm function $N(a+bi) = a^2+b^2$. Using $N(z_1 z_2) = N(z_1)N(z_2)$ show that $z = 2+i \in \mathbb{Z}[i]$ is irreducible (i.e. $z = x \cdot y$ in $\mathbb{Z}[i]$ can only happen if x or y is a unit in $\mathbb{Z}[i]$).

⑤ Using the previous problem and Euclidean Divison show that $\mathbb{Z}[i]/(2+i)$ is a field with 5 elements. Conclude that $\mathbb{Z}[i]/(2+i)$ is isomophic to $\mathbb{Z}_5$.

⑥ Show that 7 is irreducible in $\mathbb{Z}[i]$ and that $\mathbb{Z}[i]/(7)$ is a field with 49 elements