Solutions to homework 9

Wednesday, December 4, 2019 9:43 AM

① Monic irreducible polynomials of degree 1 are $x, x-1, x+1$. Divide out by those:

$$\frac{x^9-x}{x(x-1)(x+1)} = \frac{x^8-1}{x^2-1} = \frac{(x^4+1)(x^4-1)}{x^2-1} = (x^4+1)(x^2+1)$$

We see that x^2+1 is monic and irreducible (no roots in $\mathbb{F}_3$), and expect (x^4+1) to split into a pair of degree 2 irreducibles. Such irreducibles would be of the form $x^2+ax\pm1$ (since $x=0$ should not be a root). There is a total of 6 possibilities but three are reducible - $(x+1)^2, (x-1)^2, (x+1)(x-1)$. Eliminating those we are left with $x^2+1,\ x^2-x-1,\ x^2+x-1$.

So $x^9-x = x(x-1)(x+1)(x^2+1)(x^2-x-1)(x^2+x-1)$

② $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ iff $n|m$ so $\mathbb{F}_{64}$ has subfields $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8$. If $\mathbb{F}_2(\alpha) \neq \mathbb{F}_{64}$ it must be one of those smaller subfields. So $\mathbb{F}_2(\alpha)=\mathbb{F}_{64}$ precisely when $\alpha \notin \mathbb{F}_4 \cup \mathbb{F}_8 \cup \mathbb{F}_2$.

Since $\mathbb{F}_4 \cap \mathbb{F}_8 = \mathbb{F}_2$ (intersection is also a subfield) we find that the size of $\mathbb{F}_{64} \setminus (\mathbb{F}_4 \cup \mathbb{F}_8)$ is $64-4-8+2=54$

③ We can think of $\mathbb{F}_4$, resp. $\mathbb{F}_{16}$, as the set of solutions to $x^4-x=0$, resp $x^{16}-x=0$, in $\overline{\mathbb{F}_2}$.

of solutions to $x^4 - x = 0$, resp $x^{16} - x = 0$, in $\overline{\mathbb{F}}_2$. Eliminating the case $x=0$ we get equations $x^3 = 1$ (defining $\mathbb{F}_4^* < \overline{\mathbb{F}}_2^*$) and $x^{15} = 1$ (defining $\mathbb{F}_{16}^* < \overline{\mathbb{F}}_2^*$). But if $x^{15} = 1$ and $y = x^5$ then $y^3 = 1$. So if $x \in \mathbb{F}_{16}^*$ then $y = x^5 \in \mathbb{F}_4^*$, as required

4 If $2+i = z_1 z_2$ then $N(2+i) = N(z_1)N(z_2)$ so $5 = N(z_1)N(z_2)$. Since $N(z) \in \mathbb{Z}^{\geq 0}$ we have either $N(z_1) = 1$ or $N(z_2) = 1$. Since $N(a+bi) = a^2 + b^2$, $N(z) = 1$ happens only for $z = \pm 1, \pm i$. So either z_1 or z_2 must be a unit and $2+i$ is irreducible

5 We want to construct a surjective ring homomorphism $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_5$ with kernel $2+i$. Since $i^2 = -1$ in $\mathbb{Z}[i]$, we would have $\varphi(i)^2 \equiv -1 \pmod 5$. So $\varphi(i) = \pm 2$. Then $\varphi(a+bi) = a \pm 2b$. Since we want $2+i \in \operatorname{Ker}\varphi$ we choose $\varphi(i) = -2$. Then $\varphi(a+bi) = 0 \iff a - 2b = 0$
$a = 2b$ so $\operatorname{Ker}\varphi = \{2b + bi\} = (2+i)$

By the first isomorphism Thm for rings,
$$\mathbb{Z}_5 = \operatorname{Im}\varphi \cong \mathbb{Z}[i]/\operatorname{Ker}\varphi = \mathbb{Z}[i]/(2+i)$$

(6) If $7 = z_1 z_2$ then $49 = N(7) = N(z_1) N(z_2)$.
As in problem 4, $N(z_i) = 1$ implies that z_i is a unit. But $N(z_i) = 7$ would mean that $a^2 + b^2 = 7$ which has no integral solutions. So either z_1 or z_2 must be a unit and hence 7 is irreducible

We can identify $\mathbb{Z}[i]/(7)$ with $\mathbb{Z}_7[x]/(x^2+1)$

$$a + bi \longrightarrow a + bx \pmod{x^2+1}$$

Since x^2+1 is irreducible in $\mathbb{Z}_7[x]$ (no solutions for $x^2 \equiv -1 \pmod 7$), the quotient $\mathbb{Z}_7[x]/(x^2+1)$ is a field with 49 elements, as required.