DMath_U10_bf

10.5

Let $F = \mathbb{Z}_5[x]_{x^2+4x+1}$

(a) Prove that F is a field.

Proof:
$\mathbb{Z}_5$ is a field, since 5 is prime. (Theorem 5.23.)
Now, since we have shown $\mathbb{Z}_5$ to be a field, it remains to show that the polynomial $x^2 + 4x + 1$ on $\mathbb{Z}_5$ is irreducible (Theorem 5.37.). To do this, we must prove that $x^2 + 4x + 1$ has no roots in $\mathbb{Z}_5$.
Since

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$

we do this:

$$\begin{aligned} x = 0 &\implies 0^2 + 4(0) + 1 \not\equiv_5 0 \\ x = 1 &\implies 1^2 + 4(1) + 1 \not\equiv_5 0 \\ x = 2 &\implies 2^2 + 4(2) + 1 \not\equiv_5 0 \\ x = 3 &\implies 3^2 + 4(3) + 1 \not\equiv_5 0 \\ x = 4 &\implies 4^2 + 4(4) + 1 \not\equiv_5 0 \end{aligned}$$

→ you should evaluate these to explicitly show they are nonzero mod 5. -0.5

$\frac{0.5}{1.5}$

which concludes the proof, as the polynomial $x^2 + 4x + 1$ is congruent to zero over no element in the field $\mathbb{Z}$.
□

↪ To apply Corollary 5.30, you must note that x^2+4x+1 has degree 2. -0.5

(b) Prove that $F^* = \langle x + 3 \rangle$

Proof:
To prove that $F^* = \langle x + 3 \rangle$, we need to show two things:

→ This is not the definition of $\langle x+3 \rangle$. Every element in F^* must be represented by $(x+3)^a$ for some $a \in \mathbb{Z}$.

1. $F^* \subseteq \langle x + 3 \rangle$
   Every nonzero element in F can be represented as $a(x + 3) + b$, where $a, b \in \mathbb{Z}_5$, and a is not congruent to 0. This is because $x^2 + 4x + 1$ is irreducible in $\mathbb{Z}_5[x]$. Let $f(x) = a(x + 3) + b$ be an arbitrary nonzero element in F^*. We need to show that $f(x)$ can be generated by $\langle x + 3 \rangle$. Consider the polynomial $g(x) = x + 3$. Notice that $g(x)$ generates the ideal $\langle x + 3 \rangle$. Therefore, any multiple of $g(x)$ is in $\langle x + 3 \rangle$. Since $f(x)$ is a multiple of $g(x)$, we can conclude that $f(x) \in \langle x + 3 \rangle$, and thus, $F^* \subseteq \langle x + 3 \rangle$.
   this is not true.
2. $\langle x + 3 \rangle \subseteq F^*$
   Consider an arbitrary element $h(x) = c(x + 3)$ where $c \in \mathbb{Z}_5$ and c is not congruent to 0. This element is in $\langle x + 3 \rangle$. Since $x^2 + 4x + 1$ is irreducible, $c(x + 3)$ is nonzero, and thus, $h(x) \in F^*$. This is because every nonzero element in F can be expressed as $a(x + 3) + b$. Therefore, $\langle x + 3 \rangle \subseteq F^*$.
   X

Combining both steps, we can conclude that $F^* = \langle x + 3 \rangle$, and we have shown that every nonzero element in F can be generated by $\langle x + 3 \rangle$.
□

$\frac{0}{5}$

(c) Write $a(y) = (2x + 3)y^2 + (2x + 1)y + 1 \in F[y]$ as a product of irreducible polynomials.
Hint: $2x + 1 \equiv_{x2+4x+1} 2(x + 3) \in \mathbb{Z}_5[x]$.

Proof:
The given polynomial is $a(y) = (2x + 3)y^2 + (2x + 1)y + 1$. Using the hint, we substitute $(2x + 1)$ with $(2(x + 3))$:

$a(y) = (2(x + 3))y^2 + (2(x + 3))y + 1$

Factoring out the common factor $(2(x + 3))$:

$a(y) = 2(x + 3)(y^2 + y) + 1$

Factoring the quadratic $(y^2 + y)$ over $\mathbb{Z}_5$:
$y^2 + y = y(y+1)$

Substituting this back into the expression:
$a(y) = 2(x+3)y(y+1) + 1$

So, the irreducible factorization of $a(y)$ $F[y]$ is:
$a(y) = (2(x+3)) \cdot y \cdot (y+1) + 1$

X This is not a product of factors (you add +1 at the end)

$\frac{0}{1.5}$

The irreducible polynomials are $2(x+3)$, y, and $y+1$.
$\square$

$\frac{0.5}{8}$