Solutions 09

1. *i.* Determine all of the monic irreducible polynomials of degree 3 over $\mathbb{F}_3$.
ii. Prove that
$$\frac{\mathbb{F}_3[x]}{\langle x^3 - x - 1\rangle} \cong \frac{\mathbb{F}_3[x]}{\langle x^3 - x^2 + x + 1\rangle}\,.$$

Solution.
i. The seive of Eratosthenes gives

$x-1$	x	$x+1$	x^2-x-1	~~x^2-x~~
~~x^2-x+1~~	~~x^2-1~~	~~x^2~~	x^2+1	x^2+x-1
~~x^2+x~~	~~x^2+x+1~~	x^3-x^2-x-1	~~x^3-x^2-x~~	~~x^3-x^2-x+1~~
~~x^3-x^2-1~~	~~x^3-x^2~~	x^3-x^2+1	~~x^3-x^2+x-1~~	~~x^3-x^2+x~~
x^3-x^2+x+1	x^3-x-1	~~x^3-x~~	x^3-x+1	~~x^3-1~~
~~x^3~~	~~x^3+1~~	~~x^3+x-1~~	~~x^3+x~~	~~x^3+x+1~~
~~x^3+x^2-x-1~~	~~x^3+x^2-x~~	x^3+x^2-x+1	x^3+x^2-1	~~x^3+x^2~~
~~x^3+x^2+1~~	x^3+x^2+x-1	~~x^3+x^2+x~~	~~x^3+x^2+x+1~~	

so the 8 monic irreducible polynomials of degree 3 in $\mathbb{F}_3[x]$ are
$$\begin{array}{cccc} x^3 - x^2 + 1 & x^3 - x^2 - x - 1 & x^3 - x - 1 & x^3 - x^2 + x + 1 \\ x^3 - x + 1 & x^3 + x^2 - x + 1 & x^3 + x^2 - 1 & x^3 + x^2 + x - 1\,. \end{array}$$

ii. Consider the ring homomorphism
$$\varphi\colon \mathbb{F}_3[x] \to \frac{\mathbb{F}_3[x]}{\langle x^3 - x^2 + x + 1\rangle}$$
defined by $\varphi(x) := x^2 + x$. Since we have
$$\begin{aligned} -(x^2+x)^2 &= -x^4 - 2x^3 - x^2 = -x^4 + x^3 - x^2 \\ &= -x(x^3 - x^2 + x + 1) + x \\ (x^2+x)^2 + (x^2+x) &= x^4 + 2x^3 + 2x^2 + x = x^4 - x^3 - x^2 + x \\ &= x(x^3 - x^2 + x + 1) + x^2 \end{aligned}$$
in $\mathbb{F}_3[x]$, we see that $\varphi(-x^2) = x$ and $\varphi(x^2 + x) = x^2$. As the 27 polynomials in the $\mathbb{F}_3$-span of $\{1, x, x^2\}$ form a complete set of representatives for the cosets of $\langle x^3 - x^2 + x + 1\rangle$, we see that φ is surjective. Moreover, we have
$$\begin{aligned} (x^2+x)^3 - (x^2+x) - 1 &= x^6 + 3x^5 + 3x^4 + x^3 - x^2 - x - 1 \\ &= x^6 + x^3 - x^2 - x - 1 \\ &= x^6 + x^3 + 2x^2 - x - 1 \\ &= (x^3 + x^2 - 1)(x^3 - x^2 + x + 1) \end{aligned}$$
in $\mathbb{F}_3[x]$, so $\langle x^3 - x - 1\rangle \subseteq \operatorname{Ker}(\varphi)$. Part *i* shows that the polynomial $x^3 - x - 1$ is irreducible in $\mathbb{F}_3[x]$ which implies that the ideal $\langle x^3 - x - 1\rangle$ is maximal and $\langle x^3 - x - 1\rangle = \operatorname{Ker}(\varphi)$. Thus, the map φ induces a ring isomomorphism from the quotient $\mathbb{F}_3[x]/\langle x^3 - x - 1\rangle$ to $\mathbb{F}_3[x]/\langle x^3 - x^2 + x + 1\rangle$. $\square$

2. Factor x^4+1 into irreducibles in $\mathbb{F}_2[x]$, $\mathbb{F}_7[x]$, $\mathbb{F}_{13}[x]$, $\mathbb{F}_{17}[x]$, and $\mathbb{Q}[x]$.

Solution. In $\mathbb{F}_2[x]$, we have $(x+1)^4 = x^4+4x^3+6x^2+4x+1 = x^4+1$ and $x+1$ is clearly irreducible in $\mathbb{F}_2[x]$.

In $\mathbb{F}_7[x]$, we have $(x^2+3x+1)(x^2-3x+1) = x^4-7x^2+1 = x^4+1$. Evaluating these quadratic polynomials at each element of $\mathbb{F}_7$ gives

x	0	1	2	3	4	5	6
x^2+3x+1	1	5	4	5	1	6	6
x^2-3x+1	1	6	6	1	5	4	5

As these quadratic polynomials have no roots in $\mathbb{F}_7$, they are irreducible in $\mathbb{F}_7[x]$.

In $\mathbb{F}_{13}[x]$, we have $(x^2-5)(x^2+5) = x^4-25 = x^4+1$. Evaluating these quadratic polynomials at each element of $\mathbb{F}_{13}$ gives

x	0	1	2	3	4	5	6	7	8	9	10	11	12
x^2-5	8	9	12	4	11	7	5	5	7	1	4	12	9
x^2+5	5	6	9	1	8	4	2	2	4	8	1	9	6

As these quadratic polynomials have no roots in $\mathbb{F}_{13}$, we see that they are irreducible in $\mathbb{F}_{13}[x]$.

In $\mathbb{F}_{17}[x]$, we have

$$(x-8)(x+8)(x-2)(x+2) = (x^2-13)(x^2-4) = x^4-17x^2+52 = x^4+1\,.$$

The linear polynomials are clearly irreducible in $\mathbb{F}_{17}[x]$.

The irreducible factorization of x^4+1 in $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$ are the equal. Since $m^4 > 0$ for any nonzero integer m, we see that x^4+1 does not have a linear factor in $\mathbb{Z}[x]$. Suppose there exists integers a, b, c, and d such that

$$\begin{aligned} x^4+1 &= (x^2+ax+b)(x^2+cx+d) \\ &= x^4+(a+c)x^3+(b+d+ac)x^2+(ad+bc)x+bd\,. \end{aligned}$$

It follows that $a+c=0$, $b+d+ac=0$, $ad+bc=0$ and $bd=1$. From these equations, we obtain $b=d=\pm1$, $a=-c$ and $c^2=\pm2$ which is impossible because $c\in\mathbb{Z}$. Thus, x^4+1 has no quadratic factors in $\mathbb{Z}[x]$. Since x^4+1 has no factors in $\mathbb{Z}[x]$, we conclude that it is irreducible in x^4+1. □

Remark. For every prime integer p, the polynomial x^4+1 factors in $\mathbb{F}_p[x]$, but it is irreducible in $\mathbb{Z}[x]$.

3. Consider $f := xz - yw$ in $\mathbb{Z}[w,x,y,z]$.

i. Prove that $\langle f\rangle$ is a prime ideal in $\mathbb{Z}[w,x,y,z]$.

ii. Prove that $\mathbb{Z}[w,x,y,z]/\langle f\rangle$ is not a unique factorization domain.

Solution.

i. Because the ring $\mathbb{Z}[x,y,z,w]$ is a unique factorization domain, it suffices to show that the polynomial $f = xz - yw$ is irreducible. Suppose that

$$wz - xy = g(x,y,z,w)\cdot h(x,y,z,w)$$

for some g and h in $\mathbb{Z}[w,x,y,z]$ having positive degree. As f is homogeneous of degree 2, it follows that g and h are homogeneous of degree 1, so

$$g = Ax + By + Cz + Dw \qquad \text{and} \qquad h = Ex + Fy + Gz + Hw$$

for some integers $A, B, \dots, H$. Hence, we obtain

$$\begin{aligned} xz - yw &= g(x,y,z,w) \cdot h(x,y,z,w) \\ &= AEx^2 + (AF+BE)xy + (AG+CE)xz + (AH+DE)xw \\ &\quad + BFy^2 + (BG+CF)yz + (BH+DF)yw + CGz^2 \\ &\quad + (CH+DG)zw + HDw^2 . \end{aligned}$$

Since $AE = 0$ and $AG + CE = 1$ exactly one of A and E is zero. If $A = 0$, then the equation $0 = AF + BE = BE$ implies that $B = 0$ and the equation $0 = AH+DE = DE$ implies that $D = 0$. However, this means $-1 = BH+DF = 0$ which is a contradiction. If $E = 0$ then the equation $0 = AF+BE = AF$ implies that $F = 0$ and the equation $0 = AH + DE = AH$ implies that $H = 0$. However, this means $-1 = BH + DF = 0$ which is again a contradiction. Therefore, the polynomial $xz - yw$ is irreducible.

ii. First, we claim that the coset $x + \langle f \rangle$ in the quotient ring $\mathbb{Z}[x,y,z,w]/\langle f \rangle$ is irreducible. Suppose there exists polynomials g and h in $\mathbb{Z}[w,x,y,z]$ such that $x + \langle f \rangle = (g + \langle f \rangle)(h + \langle f \rangle)$. Hence, we have $x - g\,h \in \langle f \rangle$. Decomposing the polynomials g and h into homogeneous parts, we have

$$g = \sum_{i=0}^{d} g_i \qquad \text{and} \qquad h = \sum_{j=0}^{\ell} h_j .$$

We may assume that, for any nonnegative integers i and j, neither g_i nor h_j belong to the principal ideal $\langle f \rangle$. Since f is homogeneous, it follows that each homogeneous part of $x - g\,h$ also belongs to the ideal $\langle f \rangle$. If $\max(d,\ell) > 1$, then the top degree part of $x - g\,h$ is $g_d\,h_\ell \in \langle f \rangle$. Because the ideal $\langle f \rangle$ is prime, we have either $g_d \in \langle f \rangle$ or $h_\ell \in \langle f \rangle$ contradicting our assumptions. Thus, we see that $\max(d,\ell) \leqslant 1$. The degree 0 part of $x - g\,h$ is $g_0\,h_0$. Since f has degree 2, the relation $g_0 h_0 \in \langle f \rangle$ implies that either $g_0 = 0$ or $h_0 = 0$. Without loss of generality, we may assume $g_0 = 0$. Hence, the degree 1 part of $x - g\,h$ equals $x - g_1\,h_0$. Because $x - g_1\,h_0 \in \langle f \rangle$, we have $x - g_1\,h_0 = 0$ and $g_1 = \pm x$ and $h_0 = \mp 1$. Lastly, degree 2 part of $x - g\,h$ equals $g_1\,h_1 = \pm x\,h_1 \in \langle f \rangle$ which implies that $h_1 = 0$. We conclude that $g = \pm x$ and $h = \mp 1$, so the image of x in the quotient $\mathbb{Z}[x,y,z,w]/\langle f \rangle$ is irreducible.

By symmetry, the images of x, y, z, and w in the quotient $\mathbb{Z}[x,y,z,w]/\langle f \rangle$ are distinct and irreducible. Hence, the equation $xz = yw$ in this quotient ring gives two distinct factorizations of an element into irreducibles. □