December 8, 2025

Problem Set 12 Solutions

Exercise 1. Find the units and irreducible elements in the ring $\mathbb{Z}/4\mathbb{Z}$.

Solution 1. Consider the multiplication table in the ring $\mathbb{Z}/4\mathbb{Z}$:

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

.

This shows that the elements $\bar{1}, \bar{3} \in \mathbb{Z}/4\mathbb{Z}$ are the units. The element $\bar{2} = \bar{2} \cdot \bar{3} = \bar{2} \cdot \bar{1}$, therefore it is always a product of $\bar{2}$ and a unit. Therefore, $\bar{2}$ irreducible.

Exercise 2. (a) Let K be a field and $p(X) \in K[X]$. Show that if for $\alpha \in K$, we have $p(\alpha) = 0$, then $X - \alpha$ divides p.

(b) Let $p(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$, $a_n \neq 0$. Suppose that $\frac{r}{s} \in \mathbb{Q}$ is a root of $p(X)$, such that $\gcd(r, s) = 1$, so that we have $p(\frac{r}{s}) = 0$. Show that $s|a_n$ and $r|a_0$ in $\mathbb{Z}$. In particular, if $p(X)$ is monic (i.e., $a_n = 1$), the only rational roots of $p(X)$ are integers. Use this property to determine which of the following polynomials are irreducible in $\mathbb{Q}[X]$.

$$X^2 - 2, \qquad X^3 + X + 1,$$
$$X^3 + 2X^2 - 3, \qquad 2X^9 - X - 1, \qquad 5X^3 - 2X^2 + 6$$

Solution 2. (a) Consider the euclidean division of the polynomial p by $(X - \alpha)$: $p = (X - \alpha)q + r$, where q, $r \in K[X]$ and either $r = 0$ or $\deg(r) < \deg(X - \alpha)$. Suppose that $r \neq 0$, then $\deg(r) = 0$ and $r = k \neq 0$ for some $k \in K$. Then, $p(\alpha) = k \neq 0$, a contradiction. Therefore $X - \alpha$ divides p.

(b) Consider $p(\frac{r}{s}) = a_n(\frac{r}{s})^n + a_{n-1}(\frac{r}{s})^{n-1} + \cdots + a_0 = 0$:

- if we multiply both sides by s^n, shift the constant term to the right hand side, and factor out r on the left hand side, we have $r(a_n r^{n-1} + a_{n-1}r^{n-2}s + \cdots + a_1 s^{n-1}) = -a_0 s^n$. Therefore, since $(r, s) = 1$, $(r, s^n) = 1$ and so r must divide a_0.
- if we multiply both sides by s^n, shift the leading term to the right hand side, and factor out s. We obtain $s(a_{n-1}s^{n-1} + a_{n-2}s^{n-2}r + \cdots + a_0 r^{n-1}) = -a_n r^n$. As before, we can conclude that s must divide a_n.

Using this criteria we will check if the given polynomials are irreducible in $\mathbb{Q}[X]$. Recall that a polynomial in $\mathbb{Q}[x]$ of degree ≤ 3 is irreducible if an only if it has no roots in $\mathbb{Q}$.

- The roots of the monic polynomial $X^2 - 2$ can only be integers dividing 2 therefore $\pm 1, \pm 2$. We can easily check that these are not the roots.
- The roots of the monic polynomial $X^3 + X + 1$ can only be integers dividing 1 therefore ± 1. We have can easily check that these are not the roots.
- Suppose $p(X) = X^3 + 2X^2 - 3$ factors; then one of the factors is degree 1 and so p has a root in $\mathbb{Q}$. Suppose $\frac{r}{s} \in \mathbb{Q}$, $(r, s) = 1$ and it is a root of $p(X) = X^3 + 2X^2 - 3$. We have that $s = 1$ and $r \in \pm 1, \pm 3$. Sinc $p(1) = 0$, $X - 1$ divides $p(X)$ and so $p(X)$ is not irreducible in $\mathbb{Q}[X]$.
- If we find a root of $p(X)$, then it is not irreducible. However, if we find no roots, we cannot conclude that the polynomial is irreducible because its degree is > 3. Suppose $\frac{r}{s} \in \mathbb{Q}$, $(r, s) = 1$ and it is a root of $2X^9 - X - 1$. We must have that $s \in \{\pm 1, \pm 2\}$ and $r = \pm 1$. Observe that $p(1) = 0$, thus by (a), $(X - 1)$ divides p and so p is not irreducible in $\mathbb{Q}[X]$.
- We argue as for the first polynomial above, since here as well we have a polynomial of degree three. Suppose $\frac{r}{s} \in \mathbb{Q}$, $(r, s) = 1$ and it is a root of $5X^3 - 2X^2 + 6$. We must have that $s \in \{\pm 1, \pm 5\}$ and $r \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. So we need to check if there is any root of p in the set $S = \{\pm 1, \pm 2, \pm 3, \pm 6, \frac{\pm 1}{5}, \frac{\pm 2}{5}, \frac{\pm 3}{5}, \frac{\pm 6}{5}\}$. With a little bit of patience, one can see that each element of the set S is not a root of p, therefore p is irreducible.

Exercise 3. Show that the polynomial $X^3 + 462X^2 + 2433X - 67692$ is irreducible over $\mathbb{Q}$.
Hint: Use the Eisenstein criterion.

Solution 3. Let $p = 3$ and observe that p divides $462, 2433$ and 67692 but doesn't divide the coefficient of X^3. Moreover, $p^2 = 9$ doesn't divide 67692. Therefore, we can use Eisenstein Criterion to conclude that $f(X)$ is irreducible over $\mathbb{Q}$.

Exercise 4. (Chinese remainder theorem for polynomial rings). Find a polynomial $f(X) \in \mathbb{Q}[X]$ such that

$$\begin{cases} f \equiv X \pmod{X^2+1} \\ f \equiv -1 \pmod{X-1} \\ f \equiv X+2 \pmod{X^2-4}. \end{cases}$$

Solution 4. Fix $a = X^2 + 1$, $b = X - 1$ and $c = X^2 - 4$. The elements a, b, c are pairwise coprime in $\mathbb{Q}[X]$.

(a) Since a, b and c divide $m = (X^2+1)(X-1)(X^2-4)$, we have a well defined ring homomorphism:

$$\begin{aligned} \varphi : \mathbb{Q}[X]/(m) &\longrightarrow \mathbb{Q}[X]/(a) \times \mathbb{Q}[X]/(b) \times \mathbb{Q}[X]/(c) \\ [s]_c &\mapsto ([s]_a, [s]_b, [s]_c). \end{aligned}$$

Moreover a, b and c are pairwise coprime polynomials in $\mathbb{Q}[X]$, therefore by the CRT (Chinese Remainder Theorem) we know that our system has a unique solution f modulo m.

(b) We will start by solving the first two equations of the system:

$$\begin{cases} f \equiv X \pmod{a} \\ f \equiv -1 \pmod{b} \end{cases}$$

Since a and b are coprime, we know that the system has a solution modulo $d = a \cdot b = (X^2+1)(X-1)$. Observe that f is a solution if and only if there are polynomials g and h such that $f = g \cdot a + X = h \cdot b - 1$. Thus, $g \cdot a - h \cdot b = -1 - X$. One can take $g = -1$ et $h = -X$, which will give us $f = -X^2 + X - 1$. If one doesn't find g, h with a straightforward method, it's recommended using the Bézout Identity and the Extended Euclidean Algorithm.

Now, the original system is equivalent to the following one:

$$\begin{cases} f \equiv -X^2 + X - 1 \pmod{d} \\ f \equiv X + 2 \pmod{c}. \end{cases}$$

Again since c and d are coprime polynomials, by the CRT one knows that there exists a solution modulo $m = d \cdot c = a \cdot b \cdot c$. A polynomial f is a solution if there are polynomial g and h such that $f = g \cdot d - X^2 + X - 1 = h \cdot c + X + 2$. Meaning that

$$t = g \cdot d - h \cdot c, \tag{1}$$

where $t = X^2 + 3$.

Since it's hard to find straightforward g and h we will use the Bézout Identity and the Extended Euclidean Algorithm. We use them to compute z, w such that:

$$1 = w \cdot c + z \cdot d \tag{2}$$

In our case $w = -\frac{1}{15}(X^2 + 4)$ and $z = \frac{1}{15}(X + 1)$. Then, by multiplying both sides of equation (2) by $t = X^2 + 3$ we obtain:

$$t = t \cdot w \cdot c + t \cdot z \cdot d. \tag{3}$$

Therefore, comparing equation (1) and (2), one can take $g = t \cdot z$ and $h = -t \cdot w$.

Then the set of the solutions of the system of congruences is the set of all the values congruent to

$$f = -t \cdot w \cdot c + X + 2 \quad \text{modulo } m.$$

Exercise 5. Let $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ be the field of 5 elements. Use the Euclidean algorithm in $\mathbb{F}_5[x]$ to find F, the monic greatest common divisor of the given polynomials $P = 3x^5 + x + 1$ and $Q = x^2 + 3x + 1$. Then use Bezout's theorem to express F in the form $F = aP + bQ$, where $a, b \in \mathbb{F}_5[x]$.

Solution 5. By Euclidean division we find $P(x) = Q(x)(3x^3 - 4x^2 - x + 2) + (x - 1)$, and $Q(x) = (x-1)(x+4)$. Therefore, $x - 1$ is the monic $\gcd(P(x), Q(x))$ over $\mathbb{F}_5$. Reading the Euclidean algorithm backwards we find $(x-1) = P(x) - (3x^3 - 4x^2 - x + 2)Q(x)$.