December 16, 2024

Problem Set 13 Solutions

Exercise 1. Let $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ be the field of 3 elements . Let $I = ((X^2+1))$ be the ideal in $\mathbb{F}_3[X]$.

(a) Show that X^2+1 is irreducible in $\mathbb{F}_3[X]$ and deduce that the quotient ring $\mathbb{F}_3[X]/I$ is a field.

(b) How many elements are there in this field? List all the elements.

(c) Show that $g(X) = 2X+1$ is a generator of the multiplicative group of units of this field.

Solution 1. (a) The polynomial $f(X) = X^2+1$ is irreducible in $\mathbb{F}_3[X]$ if and only if it has no roots in $\mathbb{F}_3$ (by degree). Then in $\mathbb{F}_3$ we have:

$$f(0) = 1, \quad f(1) = 2, \quad f(2) = 2.$$

Therefore $f(X)$ is irreducible in $\mathbb{F}_3[X]$. We can conclude by the theorem from the course that the quotient ring $\mathbb{F}_3[X]/I$ is a field.

(b) This field has 9 elements, $\mathbb{F}_3[X]/I = \{[0]_I, [1]_I, [2]_I, [X]_I, [2X]_I, [X+1]_I, [X+2]_I, [2X+1]_I, [2X+2]_I\}$. How to see this: let $r(X) \in \mathbb{F}_3[X]$. If $\deg(r) \geq 2$, then we can divide by X^2+1 and write $r(X) = q(X)(X^2+1) + r_0(X)$ where $r_0(X)$ is of degree at most 1 or the 0 polynomial. Hence in the quotient ring, $r(X)$ is congruent to $r_0(X)$ modulo the ideal (X^2+1). So the distinct elements come from the congruence classes of the form, $[AX+B]_I$, for $A, B \in \mathbb{F}_3$.

(c) We compute the powers of the polynomial $2X+1$ modulo the ideal $((X^2+1))$:

$$[2X+1], \quad [(2X+1)]^2 = [X], \quad [(2X+1)]^3 = [X+1], \quad [(2X+1)]^4 = [2], \quad [(2X+1)]^5 = [X+2]$$

$$[(2X+1)]^6 = [2X], \quad [(2X+1)]^7 = [2X-1], \quad [(2X+1)]^8 = [1].$$

Exercise 2. Let $K = \mathbb{Q}[X]/(X^2+2X+3)$. Denote by α the class of X in K.

(a) Show that K is a field.

(b) Show that $2\alpha - 1$ is nonzero and compute its inverse in K.

Solution 2. (a) If F is a field, the quotient ring $F[X]/(f(X))$ is a field if and only if the polynomial $f(X)$ is irreducible in $F[X]$. The discriminant of X^2+2X+3 is $2^2 - 4 \times 3 = -8 < 0$. Therefore the polynomial X^2+2X+3 has no roots in $\mathbb{Q}$, and it is of degree 2, and so irreducible in $\mathbb{Q}[X]$. Therefore K is a field.

(b) Since $2\alpha - 1 = [2X-1]$ and this polynomial is not divisible by X^2+2X+3, it is a nonzero element in K. We use Bezout's identity to find $f(X), g(X)$ such that $f(X)(2X-1) + g(X)(X^2+2X+3) = 1$ in $\mathbb{Q}[X]$. Then $[f(x)]$ is the inverse of $[2X-1]$ in K. The Euclidean division for $2X-1, X^2+2X+3$ gives:

$$X^2+2X+3 = (\frac{1}{2}X + \frac{5}{4})(2X-1) + \frac{17}{4}.$$

Therefore we have in K:

$$(\frac{1}{2}\alpha + \frac{5}{4})(2\alpha - 1) + \frac{17}{4} = 0,$$

and

$$-\frac{4}{17}(\frac{1}{2}\alpha + \frac{5}{4})(2\alpha - 1) = 1,$$

which implies $(2\alpha-1)^{-1} = -\frac{2}{17}\alpha - \frac{5}{17}$.

Exercise 3. Let $K = \mathbb{F}_7[X]/(X^3-2)$

(a) Show that the polynomial $P(X) = X^3 - 2$ is irreducible over $\mathbb{F}_7$.

(b) Decompose the polynomial (X^3-2) into irreducible factors over K.

(d) Give a basis of K as a vector space over $\mathbb{F}_7$.

(e) Find the number of elements of K.

Solution 3. (a) For a polynomial of degree 3 it is enough to show that it has no roots in $\mathbb{F}_7$. We have $P(0) = 5, P(1) = 6, P(2) = 6, P(3) = 4, P(4) = 2, P(5) = 3$ and $P(6) = 4$.

(b) Let $K = \mathbb{F}_7[X]/(X^3 - 2)$. Let β be the class of X in K, $\beta = [X]_{(X^3-2)}$. Then in K, $\beta^3 = 2$ and therefore the polynomial $X^3 - 2$ has a linear factor $X - \beta$ in the ring $K[X]$. Using the fact that in $\mathbb{F}_7$, we have $2^3 = 1$, we obtain that 2β is another root and $(X - 2\beta)$ is also a factor. The third root is 4β because we have $4^3 = 1$. Finally we have $X^3 - 2 = (X - \beta)(X - 2\beta)(X - 4\beta)$.

(d) Let $\beta = [X]_{(P)} \in K$. Then K is a 3-dimensional vector space over $\mathbb{F}_7$ with basis $\{1, \beta, \beta^2\}$

(e) Since each element of K can be written uniquely as $a_1 \cdot 1 + a_2 \cdot \beta + a_3 \cdot \beta^2$, for $a_i \in \mathbb{F}_7$, K has 7^3 elements.

Exercise 4. (a) Find an explicit isomorphism between the rings $\mathbb{F}_2[x]/(x^2)$ and $\mathbb{F}_2[x]/(x^2 + 1)$. Are they also isomorphic to the ring $\mathbb{Z}/4\mathbb{Z}$? Is any of these rings an integral domain?

(b) Show that the ring $\mathbb{F}_2[x]/(x^2+x+1)$ is a field of 4 elements and therefore is not isomorphic to $\mathbb{F}_2[x]/(x^2)$ or $\mathbb{Z}/4\mathbb{Z}$.

(c) Check that the group of units of the field $\mathbb{F}_2[x]/(x^2 + x + 1)$ is cyclic and find a generator.

(d) The fields $K_1 = \mathbb{F}_2[x]/(x^3 + x + 1)$ and $K_2 = \mathbb{F}_2[x]/(x^3 + x^2 + 1)$ are isomorphic. Find an explicit isomorphism between them.

Solution 4. (a) We have $\mathbb{F}_2[x]/(x^2) = \{0, 1, \mu, \mu + 1\}$, where $\mu = [x]_{(x^2)}$ is the congruence class of the element x modulo the ideal (x^2). Then $\mu^2 = 0, (\mu+1)^2 = 1, \mu(\mu+1) = \mu$. We also have $(\mu+1)+\mu = 1$. On the other hand, the ring $\mathbb{F}_2[x]/(x^2 + 1) = \{0, 1, \nu, \nu + 1\}$, where $\nu = [x]_{(x^2+1)}$ is the congruence class of the element x modulo the ideal $(x^2 + 1)$. Then we have $\nu^2 = 1, (\nu + 1)^2 = 0, \nu(\nu + 1) = \nu + 1$, and $\nu + (\nu + 1) = 1$. Clearly the map $f : \mathbb{F}_2[x]/(x^2) \to \mathbb{F}_2[x]/(x^2 + 1)$, $f(0) = 0, f(1) = 1, f(\mu) = \nu + 1, f(\mu + 1) = \nu$ is a ring isomorphism, because it respects both ring operations.
Note that the characteristic of both rings $\mathbb{F}_2[x]/(x^2)$ and $\mathbb{F}_2[x]/(x^2 + 1)$ is 2: we have $1 + 1 = 0$ in both rings. However, the characteristic of the ring $\mathbb{Z}/4\mathbb{Z}$ is 4. Therefore the they cannot be isomorphic to $\mathbb{Z}/4\mathbb{Z}$. None of these rings are integral domains: we have $\mu^2 = 0 \in \mathbb{F}_2[x]/(x^2)$, $(\nu + 1)^2 = 0 \in \mathbb{F}_2[x]/(x^2 + 1)$, and $2^2 = 0 \in \mathbb{Z}/4\mathbb{Z}$.

(b) The polynomial $x^2 + x + 1$ of degree 2 is irreducible over $\mathbb{F}_2$ since it has no roots in $\mathbb{F}_2$. Therefore the quotient ring $\mathbb{F}_2[x]/(x^2+x+1)$ is a field. Since the degree of the polynomial generating the ideal is 2, this field has $2^2 = 4$ elements. It is clearly not isomorphic to either of the rings $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{F}_2[x]/(x^2)$, or $\mathbb{F}_2[x]/(x^2+1)$ because all of them have zero divisors.

(c) Denote by α the class of x in $\mathbb{F}_2/(x^2+x+1)$. Then we have $\{0, 1, \alpha, \alpha+1\}$ the elements of the field $\mathbb{F}_2/(x^2+x+1)$. Consider the powers of α: $\alpha^2 = \alpha + 1$, $\alpha^3 = 2\alpha + 1 = 1$, therefore the group of units $(\mathbb{F}_2/(x^2 + x + 1))^* \simeq C_3$ and we can take α to be its generator.

(d) Denote by ν and μ the class of x in K_1 and K_2 respectively. Both fields have $2^3 = 8$ elements. We can write the powers of μ in the group of units $(K_2)^*$:

$$\{\mu,\ \mu^2,\ \mu^2 + 1,\ \mu^2 + \mu + 1,\ \mu + 1,\ \mu^2 + \mu,\ 1\}$$

On the other hand, we can write the powers of $\nu + 1$ in the group of units $(K_1)^*$:

$$\{\nu + 1,\ \nu^2 + 1,\ \nu^2,\ \nu^2 + \nu + 1,\ \nu,\ \nu^2 + \nu,\ 1\}.$$

The map $\Phi : K_2 \to K_1$ such that $\Phi(\mu) = \nu + 1$ can be extended to an isomorphism of the multiplicative groups of units by setting $\Phi(\mu^k) = (\nu + 1)^k$. Then it is easy to check directly that $\Phi(\mu^k + \mu^m) = (\nu + 1)^k + (\nu + 1)^m$ for any $0 \le m, n \le 7$, therefore $\Phi(0) = 0$ extends the map to an isomorphism of fields.