ADVANCED MATHEMATICS

Rings and Fields: Polinomials and Finite Fields II

1. a) Prove that $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$ and that $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{C}$.
   b) Show that in $\mathbb{Z}_3$ there is no element α such that $\alpha^2 = 2$. Define $\mathbb{Z}_3[\alpha]$, with $\alpha^2 = 2$, in a similar way to $\mathbb{Q}[\sqrt{2}]$. Prove that $\mathbb{Z}_3[\alpha]$ is a field. How many elements are there in $\mathbb{Z}_3[\alpha]$?
   c) Show that $x^2 - 2 \in \mathbb{Z}_3[x]$ is irreducible. Is $x^2 - 2$ irreducible in $\mathbb{Z}_3[\alpha][x]$?

2. a) Find all the monic irreducible polynomials of degrees 2 and 3 in $\mathbb{Z}_2[x]$ and $\mathbb{Z}_3[x]$, and of degree 2 in $\mathbb{Z}_5[x]$.
   b) Decompose the polynomial $x^4 + 1$ in a product of irreducible polynomials in $\mathbb{Z}_5[x]$.

3. Decompose in irreducible factors the polynomials $f = x^6 - 1$ and $g = x^6 + 1$ as members of the rings $\mathbb{R}[x]$ and $\mathbb{C}[x]$.

4. Factorize $f = 4x^2 - 4x + 8$ as a product of irreducibles in $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ and $\mathbb{Z}_{11}[x]$.

5. Decompose in irreducible factors the polynomial $f = x^4 + 1$ in the rings $\mathbb{Z}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}_2[x]$, $\mathbb{Z}_3[x]$ and $\mathbb{Z}_7[x]$.

6. Let $f = a_n x^n + a_{n-1}x^{n-1} + ... + a_0 \in \mathbb{Z}[x]$ a polynomial of degree n with $a_0 \neq 0$. Show that if p, q are two relative prime integers then $f(p/q) = 0$ implies that $p|a_0$ and $q|a_n$. Using this result, factorize $f = 3x^3 + 4x^2 + 2x - 4$ in $\mathbb{Q}[x]$.

7. Study irreducibility in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$ of the polynomials:
   a) $f_1 = x^3 + 3x^2 + 3x + 9$ b) $f_2 = 5x^{10} + 10x^7 + 20x^3 + 10$ c) $f_3 = x^3 + 5x^2 + 3x + 35$
   d) $f_4 = -x^7 + 25x^2 - 15x + 10$ e) $f_5 = 7x^3 + 6x^2 + 4x + 6$ f) $f_6 = 9x^4 + 4x^3 - 3x + 7$.

8. Show that the set $I := \{f(x) \in \mathbb{Z}[x] \mid f(0) \in 3\mathbb{Z}\}$ is an ideal.
   (a) Find two elements in $\mathbb{Z}[x]$ that generate I. Is I a principal ideal?
   (b) Let $\psi : \mathbb{Z}[x] \to \mathbb{Z}_3$ be the mapping defined by $f(x) \mapsto f(0) \bmod 3$. Prove that ψ is an homomorphism of rings with unity. Find the kernel and image of ψ. Prove that the ring quotient: $\mathbb{Z}[x]/I$ is isomorphic to $\mathbb{Z}_3$.

9. **(*)** Let f be an irreducible polynomial in $\mathbb{Q}[x]$.
   (a) For $a \in \mathbb{C}$ consider the **evaluation homomorphism** $\mathrm{ev}_a : \mathbb{Q}[x] \to \mathbb{C}$ defined by: $h(x) \mapsto h(a)$. Prove that if $f(a) = 0$, then the kernel of ev_a is the principal ideal generated by f.
   (b) Furthermore, prove that if $g \in \mathbb{Q}[x]$ and $g(a) = 0$ then f divides g in $\mathbb{Q}[x]$.

10. **(*)** Consider the evaluation homomorphism $\mathrm{ev}_i : \mathbb{R}[x] \to \mathbb{C}$ defined by $\mathrm{ev}_i(P) = P(i)$. Find the image of ev_i. Prove that the kernel $\ker(\mathrm{ev}_i)$, is the ideal generated by the polynomial $f(x) = x^2 + 1$. Conclude that $\mathbb{R}[x]/\langle f \rangle$ is a field isomorphic to $\mathbb{C}$.

11. Decompose in irreducible factors the polynomial $f = 4x^2 - 12$ considered as an element of $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ and $\mathbb{R}[x]$. Is $\mathbb{Q}[x]/\langle f \rangle$ a field? and $\mathbb{R}[x]/\langle f \rangle$? In case of affirmative answer show its characteristic and its dimension as a vector space over $\mathbb{Q}$ and $\mathbb{R}$ respectively.

12. Is $\mathbb{Q}[x]/\langle x^2 - 5x + 6 \rangle$ a field? And $\mathbb{Q}[x]/\langle x^2 - 6x + 6 \rangle$? In the affirmative cases find its characteristic and its dimension as a vector space over $\mathbb{Q}$.

13. Study the quotient ring $\mathbb{Z}_2[x]/\langle f \rangle$, showing the number of elements and constructing the addition and multiplication tables in the following cases:
    i) $f = x^2 + 1$ ii) $f = x^2 + 2$ iii) $f = x^2 + x + 1$ iv) $f = x^3 + x + 1$ v) $f = x^3 + x^2 + 1$.
    Is some of these rings a field? In that case, find its characteristic. Which is the dimension (as vector spaces) over the field $\mathbb{Z}_2$?

14. Construct fields with 4, 8, 9 and 25 elements, showing its characteristic.

15. Find a divisor of zero in the quotient ring $A := \mathbb{Q}[x]/\langle x^3 - x^2 + x - 1\rangle$. Is $\alpha = [x]$ (the class of x in A) a unit in this ring? In the case of affirmative answer find its inverse.

16. Consider $\alpha = [x]$ as an element of $\mathbb{Z}_3[x]/(x^2 + x - 1)$. Find, if exists, the inverse of $\alpha^4 + \alpha^3 + \alpha^2 + \alpha$.

17. Let $f = x^3 + x + 1 \in \mathbb{F}[x]$ and the quotient $L = \mathbb{F}[x]/\langle f\rangle$, where $\mathbb{F}$ is a field.
(a) Analize if L is a field in the cases $\mathbb{F} = \mathbb{Z}_3$ and $\mathbb{F} = \mathbb{Z}_5$.
(b) Denote $\alpha = [x] \in L$. In each case, study if $\alpha - 1$ has an inverse in L, and find it if it exists.

18. **(*)** Consider a prime number $n \geq 2$ and the ring quotient $A = \mathbb{Z}_n[x]/\langle x^2 - x\rangle$. Show that the mapping $f : A \to \mathbb{Z}_n \times \mathbb{Z}_n$ defined by $f(a + b[x]) = (a + b, a)$ is a ring homomorphism.

19. Analize if there are isomorphisms between the following rings:
i) $\mathbb{Z}_2 \times \mathbb{Z}_2$ ii) $\mathbb{Z}_4$ iii) $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ iv) $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ v) $\mathbb{Z}_2[x]/\langle x^3 + x^2 + 1\rangle$ vi) $\mathbb{Z}_2[x]/\langle x^2\rangle$ justifying the answers.

20. Find the unique polinomial $f(x)$ of degree less or equal 3 and with coefficients in $\mathbb{Z}_7$ such that $f(1) = 0$, $f(3) = 1$, $f(4) = 2$ and $f(6) = 0$.

21. Find the unique polinomial $f(x) \in \mathbb{Z}_3[x]$ of degree less or equal 5 such that, when it is divided by $x^3 + 2x + 1$ or by x^3 has a remainder $x^2 + x + 1$.

22. a) Consider the field of four elements $\mathbb{F}_4 = \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$. Find $[x]^{432}$. b) Consider the field of 25 elements $\mathbb{F}_{25} = \mathbb{Z}_5[x]/\langle x^2 + 2x + 4\rangle$. Find $[x]^{1300}$ and $[2x + 1]^{2281}$.