Section 2 Unique Factorization Domains

2.1. Factor the following polynomials into irreducible factors in $\mathbb{F}_p[x]$.

(a) x^3+x^2+x+1, $p=2$, **(b)** x^2-3x-3, $p=5$, **(c)** x^2+1, $p=7$

2.2. Compute the greatest common divisor of the polynomials $x^6+x^4+x^3+x^2+x+1$ and $x^5+2x^3+x^2+x+1$ in $\mathbb{Q}[x]$.

2.3. How many roots does the polynomial x^2-2 have, modulo 8?

2.4. Euclid proved that there are infinitely many prime integers in the following way: If $p_1, \ldots, p_k$ are primes, then any prime factor p of $(p_1 \cdots p_k)+1$ must be different from all of the p_i. Adapt this argument to prove that for any field F there are infinitely many monic irreducible polynomials in $F[x]$.

2.5. *(partial fractions for polynomials)*

(a) Prove that every element of $\mathbb{C}(x)$ x can be written as a sum of a polynomial and a linear combination of functions of the form $1/(x-a)^i$.

(b) Exhibit a basis for the field $\mathbb{C}(x)$ of rational functions as vector space over $\mathbb{C}$.

2.6. Prove that the following rings are Euclidean domains.

(a) $\mathbb{Z}[\omega]$, $\omega = e^{2\pi i/3}$, **(b)** $\mathbb{Z}[\sqrt{-2}]$.

2.7. Let a and b be integers. Prove that their greatest common divisor in the ring of integers is the same as their greatest common divisor in the ring of Gauss integers.

2.8. Describe a systematic way to do division with remainder in $\mathbb{Z}[i]$. Use it to divide $4+36i$ by $5+i$.

2.9. Let F be a field. Prove that the ring $F[x, x^{-1}]$ of Laurent polynomials (Chapter 11, Exercise 5.7) is a principal ideal domain.

2.10. Prove that the ring $\mathbb{R}[[t]]$ of formal power series (Chapter 11, Exercise 2.2) is a unique factorization domain.

Section 3 Gauss's Lemma

3.1. Let φ denote the homomorphism $\mathbb{Z}[x] \to \mathbb{R}$ defined by

(a) $\varphi(x) = 1+\sqrt{2}$, **(b)** $\varphi(x) = \frac{1}{2}+\sqrt{2}$.

Is the kernel of φ a principal ideal? If so, find a generator.

3.2. Prove that two integer polynomials are relatively prime elements of $\mathbb{Q}[x]$ if and only if the ideal they generate in $\mathbb{Z}[x]$ contains an integer.

3.3. State and prove a version of Gauss's Lemma for Euclidean domains.

3.4. Let x, y, z, w be variables. Prove that $xy-zw$, the determinant of a variable 2×2 matrix, is an irreducible element of the polynomial ring $\mathbb{C}[x, y, z, w]$.

3.5. **(a)** Consider the map $\psi: \mathbb{C}[x, y] \to \mathbb{C}[t]$ defined by $f(x, y) \rightsquigarrow f(t^2, t^3)$. Prove that its image is the set of polynomials $p(t)$ such that $\frac{dp}{dt}(0) = 0$.

(b) Consider the map $\varphi: \mathbb{C}[x, y] \to \mathbb{C}[t]$ defined by $f(x, y) \rightsquigarrow (t^2-t, t^3-t^2)$. Prove that $\ker\varphi$ is a principal ideal, and find a generator $g(x, y)$ for this ideal. Prove that the image of φ is the set of polynomials $p(t)$ such that $p(0) = p(1)$. Give an intuitive explanation in terms of the geometry of the variety $\{g=0\}$ in $\mathbb{C}^2$.

3.6. Let α be a complex number. Prove that the kernel of the substitution map $\mathbb{Z}[x] \to \mathbb{C}$ that sends $x \rightsquigarrow \alpha$ is a principal ideal, and describe its generator.

Section 4 Factoring Integer Polynomials

4.1. **(a)** Factor $x^9 - x$ and $x^9 - 1$ in $\mathbb{F}_3[x]$. **(b)** Factor $x^{16} - x$ in $\mathbb{F}_2[x]$.

4.2. Prove that the following polynomials are irreducible:
(a) $x^2 + 1$, in $\mathbb{F}_7[x]$, **(b)** $x^3 - 9$, in $\mathbb{F}_{31}[x]$.

4.3. Decide whether or not the polynomial $x^4 + 6x^3 + 9x + 3$ generates a maximal ideal in $\mathbb{Q}[x]$.

4.4. Factor the integer polynomial $x^5 + 2x^4 + 3x^3 + 3x + 5$ modulo 2, modulo 3, and in $\mathbb{Q}$.

4.5. Which of the following polynomials are irreducible in $\mathbb{Q}[x]$?
(a) $x^2 + 27x + 213$, **(b)** $8x^3 - 6x + 1$, **(c)** $x^3 + 6x^2 + 1$, **(d)** $x^5 - 3x^4 + 3$.

4.6. Factor $x^5 + 5x + 5$ into irreducible factors in $\mathbb{Q}[x]$ and in $\mathbb{F}_2[x]$.

4.7. Factor $x^3 + x + 1$ in $\mathbb{F}_p[x]$, when $p = 2, 3$, and 5.

4.8. How might a polynomial $f(x) = x^4 + bx^2 + c$ with coefficients in a field F factor in $F[x]$? Explain with reference to the particular polynomials $x^4 + 4x^2 + 4$ and $x^4 + 3x^2 + 4$.

4.9. For which primes p and which integers n is the polynomial $x^n - p$ irreducible in $\mathbb{Q}[x]$?

4.10. Factor the following polynomials in $\mathbb{Q}[x]$. **(a)** $x^2 + 2351x + 125$, **(b)** $x^3 + 2x^2 + 3x + 1$, **(c)** $x^4 + 2x^3 + 2x^2 + 2x + 2$, **(d)** $x^4 + 2x^3 + 3x^2 + 2x + 1$, **(e)** $x^4 + 2x^3 + x^2 + 2x + 1$, **(f)** $x^4 + 2x^2 + x + 1$, **(g)** $x^8 + x^6 + x^4 + x^2 + 1$, **(h)** $x^6 - 2x^5 - 3x^2 + 9x - 3$, **(j)** $x^4 + x^2 + 1$, **(k)** $3x^5 + 6x^4 + 9x^3 + 3x^2 - 1$, **(l)** $x^5 + x^4 + x^2 + x + 2$.

4.11. Use the sieve method to determine the primes <100, and discuss the efficiency of the sieve: How quickly are the nonprimes filtered out?

4.12. Determine:

(a) the monic irreducible polynomials of degree 3 over $\mathbb{F}_3$,

(b) the monic irreducible polynomials of degree 2 over $\mathbb{F}_5$,

(c) the number of irreducible polynomials of degree 3 over the field $\mathbb{F}_5$.

4.13. *Lagrange interpolation formula*:

(a) Let $a_0, \ldots, a_d$ be distinct complex numbers. Determine a polynomial $p(x)$ of degree n, which has $a_1, \ldots, a_n$ as roots, and such that $p(a_0) = 1$.

(b) Let $a_0, \ldots, a_d$ and $b_0, \ldots, b_d$ be complex numbers, and suppose that the a_i are distinct. There is a unique polynomial g of degree $\leq d$ such that $g(a_i) = b_i$ for each $i = 0, \ldots, d$. Determine the polynomial g explicitly in terms of a_i and b_i.

4.14. By analyzing the locus $x^2 + y^2 = 1$, prove that the polynomial $x^2 + y^2 - 1$ is irreducible in $\mathbb{C}[x, y]$.

4.15. With reference to the Eisenstein criterion, what can one say when
(a) $\overline{f}$ is constant, **(b)** $\overline{f} = x^n + \overline{b}x^{n-1}$?

4.16. Factor $x^{14} + 8x^{13} + 3$ in $\mathbb{Q}[x]$, using reduction modulo 3 as a guide.

4.17. Using congruence modulo 4 as an aid, factor $x^4 + 6x^3 + 7x^2 + 8x + 9$ in $\mathbb{Q}[x]$.