Problem set 6 : Finite Fields

---

(1) Identify the finite fields $\mathbb{Z}[i]/(1+i)$ and $\mathbb{Z}[i]/(2+i)$.

(2) Let $f(x) \in \mathbb{Z}[x]$ be irreducible of degree m. Let $f(x)$ have a root $r \in \mathbb{F}_{p^n}$. Show that the roots of $f(x)$ are precisely $r^p, r^{p^2}, \ldots, r^{p^n} = r$.

(3) Find a necessary and sufficient condition on n and m so that $\mathbb{F}_{p^n}$ is a subfield of $\mathbb{F}_{p^m}$.

(4) Show that $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = n/m$ if $m \mid n$.

(5) Factorize $x^8 - x$ into irreducible polynomials over $\mathbb{F}_2$.

(6) Let I denote the ideal $(X^3 + 2X + 1)\mathbb{F}_3[X]$ and let x denote the residue class $X + I$ in the field $K = \mathbb{F}_3[X]/I$. Show that x generates the cyclic group $K^\times$.

(7) Let I denote the ideal $(X^3+2X+2)\mathbb{F}_3[X]$ and x denote the residue class $X+I$ in the field $K = \mathbb{F}_3[X]/I$. Show that x does not generate the cyclic group $K^\times$. Find a generator of $K^\times$.

(8) Prove that the rings $\mathbb{F}_3[x]/(x^2+x+2)$ and $\mathbb{F}_3[x]/(x^2+2x+2)$ are isomorphic. Construct an isomorphism.

(9) Draw subfields lattices of the finite fields $\mathbb{F}_{3^{18}}$ and $\mathbb{F}_{2^{30}}$.

(10) Let $f(x)$ be a separable polynomial in $\mathbb{F}_p[x]$. Show that there exists an n such that $f(x) \mid x^{p^n} - x$.

(11) Show that the order of the Frobenius automorphism $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is n.

(12) Show that no finite field is algebraically closed.

(13) Show that the field $\cup_{n=0}^{\infty} \mathbb{F}_{p^{n!}}$ is an algebraic closure of $\mathbb{F}_p$.

(14) Let K and L be subfields of $\mathbb{F}_{p^n}$ having p^s and p^t elements respectively. How many elements does the field $K \cap L$ have ?

(15) Define $f : K = \mathbb{F}_{p^n} \to K$ by $f(x) = x^2$.

   (a) Show that f is surjective if $p = 2$.

   (b) Show that the number of elements in $f(K) = (p^n+1)/2$.

   (c) Let α and β be nonzero elements of K Show that there exist $x, y \in K$ such that $\alpha x^2 + \beta y^2 = -1$, first for $p = 2$ and then for $p > 2$ by counting the number of elements in the sets $\{1 + \alpha x^2 : x \in K\}$ and $\{\beta y^2 : y \in K\}$.

(16) Show that the product of nonzero elements of a finite field is -1. Deduce *Wilson's theorem:* If p is a prime number then $p \mid 1+(p-1)!$.

(17) Show that every element of a finite field K can be written as a sum of two squares in K.

(18) Let K be a finite field with q elements. Define the **zeta function**

$$Z(t) = \frac{1}{1-t} \prod_{p} \frac{1}{1-t^{\deg p}}$$

where p ranges over all monic irreducible polynomials over K. Prove that $Z(t)$ is a rational function and determine this rational function.