Finite Fields

By
Dr. Emad Bakr Al-Zangana
Seminar at
University of Mustansiriyah

4-9-2017

Questions on Finite Fields

- It is well known that the set on integers module prime number p , Z_p is field of order p. Dose there a finite field of order which is not prime?
- If there is a finite field of order not prime, what is the structure of this kind of a field?
- It is well known that Z_p has no proper subfield (prime subfield). Dose there a field with proper subfield?

Important Result over Finite Fields

*Every finite field is of prime power order and conversely, for every prime power, there exists a field whose order is exactly that prime power.

Questions about the Roots of a Polynomial

- Example: The polynomial $P(X) = X^2 - X = X(X-1)$ over Z_6 has three zeros 0, 1, 3, over Z_{12} has four zeros 0, 1, 4, 9 and over Z_7 has two roots 0, 1.
- Example: The polynomial $Q(X) = (X^2+1)^2$ has no Z_3 but it is reducible.
- If we have a polynomial *P* (X) of degree *d* . How many zeros of *P* are there?
- Can we find a set containing all zeros of *P* (X) ?
- Does for every positive integer *n* there exists an irreducible polynomial in Z_p of degree *n*?

Characteristic of a Field

- The smallest positive integer (if there is) n such that

$$\underbrace{1 + \cdots + 1}_{n} = 0$$

called the characteristic of the field(Ring) . If there is no such integer then we say that the field has characteristic zero.

- <u>Theorem:</u>

1-*The characteristic of a field is either* 0 *or a prime number* p.

2- *Every finite field has a prime characteristic .*

3- *The prime subfield is either a copy of* Z_p *or* $\mathbb{Q}$.

- Any field has prime subfield.
- Since any finite field cannot have $\mathbb{Q}$ as subfield, then must have a prime subfield of the form Z_p for some *p.*
- Any finite field may always be viewed as a finite dimensional vector space over its prime subfield. This dimension called the degree of the field.
- Theorem: *Any finite field with characteristic p has p^n elements where n is the degree of the field*. That is, any finite field is prime power.
- *Note that the theorem does not prove the existence of finite fields of these sizes. To prove existence we need to talk about irreducible polynomials.

- Since any field has no zero divisor , then any polynomial of degree *d* has at most *d* zeros(roots).

<u>Theorem:</u> *Let $Z_p[X]$ be a ring of polynomials and Q polynomial in $Z_p[X]$ of degree n. Then the residue class $Z_p/\langle Q\rangle$ is field of order $p^n \Leftrightarrow Q$ is irreducible over Z_p. This field called Galois Field and denoted by $GF(p^n)$.*

$$Z_p/\langle Q\rangle = \left\{a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} \mid Q(\theta) = 0\right\} = GF(p^n)$$

<u>Theorem:</u> (1) All the roots of Q are $\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}}$.

(2) $(GF(p^n)\setminus\{0\},.) = \langle\theta\rangle = \left\{1, \theta, \theta^2, \ldots, \theta^{n-1}\right\}$. θ called primitive and the irreducible polynomial which has θ as root called primitive polynomial.

(3) For every finite field $GF(q)$ and every positive integer *n* there exists an irreducible polynomial in $GF(q)$ over degree *n*.

- So, it clear that we need to find a primitive polynomial to construct the Galois field.
- Example:

A monic quadratic in $\mathbf{F}_3[X]$ is $X^2 + bX + c$ with $b, c \in \{0, 1, -1\}$. The reducible ones are

$$X^2,\ (X-1)^2 = X^2 + X + 1,\ (X+1)^2 = X^2 - X + 1,$$
$$X(X-1) = X^2 - X,\ X(X+1) = X^2 + X,\ (X-1)(X+1) = X^2 - 1.$$

This leaves the $9 - 6 = 3$ irreducibles:

$$X^2 + 1,\ X^2 - X - 1,\ X^2 - X + 1.$$

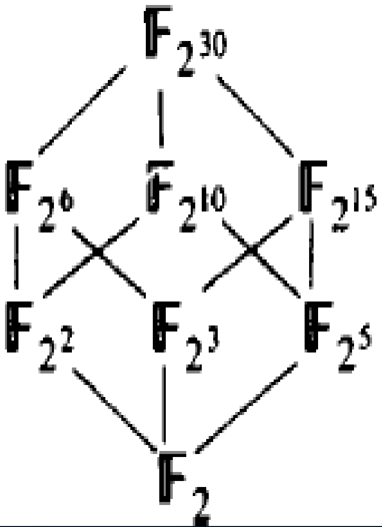
Take $X^2 + 1$ and let $\tau^2 + 1 = 0$; then $\tau^2 = -1$, and $\tau^4 = 1$. So $X^2 + 1$ is not primitive since the order of τ is not 8.

Points of $GF(9)$ using $Q(X) = X^2 - X - 1$

Power form	Polynomial form	Vector form	Order
1	1	$(1,0)$	1
σ	σ	$(0,1)$	8
σ^2	$\sigma + 1$	$(1,1)$	4
σ^3	$-\sigma + 1$	$(1,-1)$	8
σ^4	-1	$(-1,0)$	8
σ^5	$-\sigma$	$(0,-1)$	4
σ^6	$-\sigma - 1$	$(-1,-1)$	8
σ^7	$\sigma - 1$	$(-1,1)$	2

- To determined the subfields of the Galois field $GF(p^n)$ it is enough to now the divisor of *n.*
- <u>Example:</u>

The subfields of the finite field $\mathbb{F}_{2^{30}}$ can be determined by listing all positive divisors of 30. The containment relations between these various subfields are displayed in the following diagram.



Thank you

for

Your attention