Galois finite field concept

Binod Kumar*

M.Sc. Mathematics Part: I

Paper-I Advanced Abstract Algebra

Nalanda Open University, Patna

1 Finite field:

Definition 1 *A field having finite number of elements is called a finite field or a Galois finite field.*

Theorem 1 *If $\mathbb{F}$ is a finite field, then $o(\mathbb{F}) = p^n$ for some p and an integern ≥ 1.*

Let P be the prime subfied of $\mathbb{F}$.
Since $\mathbb{F}$ is finite, so is P. Therefore, $P \cong \frac{\mathbb{Z}}{\left\langle p \right\rangle}$ for some prime p.

But

$$\frac{\mathbb{Z}}{\left\langle p \right\rangle} \cong \{0, 1, 2, 3, ..., p-1\} \mod p = \mathbb{F}_p$$

$$\implies P \cong \mathbb{F}_p$$

Since $P \subseteq \mathbb{F}$, we can regard $\mathbb{F}_p \subseteq \mathbb{F}$. Now $\mathbb{F}$ is avector space over $\mathbb{F}_p$. Since $\mathbb{F}$is finite,

$$\left[\mathbb{F},\ \mathbb{F}_p\right] = n = \text{finite.}$$

Let $\{u_1, \{u_2, \{u_3, ..., \{u_n\}$ be basis of $\frac{\mathbb{F}}{\mathbb{F}_p}$.
Then

$$\mathbb{F} = \{\alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3 + ... + \alpha_n u_n \ \Big|\ \alpha_i \in \mathbb{F}_p\}$$

Now each α_i can choose in p ways and

$$\sigma\alpha_i u_i = \sigma\beta_i u_i$$

$$\implies \alpha_i = \beta_i$$

$$\therefore 0(\mathbb{F}) = p^n$$

*Corresponding author, e-mail:binodkumararyan@gmail.com, Telephone: +91-9304524851

Definition 2 *Let $\mathbb{F}$ be a finite field of $o(\mathbb{F}) = p$, and $f(x)$ is irreducible polynomial over $\mathbb{F}$ of degree n, then $\frac{\mathbb{F}(x)}{\left\langle f(x)\right\rangle}$ is a field of order p^n, it is denoted by $Gl\mathbb{F}(p^n)$, read as Galois field and $\left|Gl\mathbb{F}(p^n)\right| = p^n$ i.e.,$\mathbb{F} \cong \mathbb{Z}_p$*

Hence

$$Gl\mathbb{F}(p^n) = \frac{\mathbb{Z}_p[x]}{\left\langle f(x)\right\rangle}$$

$$= \{a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1} + \left\langle f(x)\right\rangle \;\Big|\; a_i \in \mathbb{Z}_p, \quad i = 1, 2, 3..., n-1\}$$

Theorem 2 *Construct Galois field of order 4.*

Since $\left|Gl\mathbb{F}(p^n)\right| = 2^2, \quad p = 2, \quad n = 2$

$\therefore \quad \mathbb{F} \cong \mathbb{Z}_2$

$$Gl\mathbb{F}(2^2) = \frac{\mathbb{Z}_2[x]}{\left\langle f(x)\right\rangle}$$

where $f(x) = x^2 + x + 1$ which is irreducible polynomial over $\mathbb{Z}_2$

For $f(0) = 0^2 + 0 + 1 = 1 \pmod 2$ and $f(1) = 1^2 + 1 + 1 = 1 \pmod 2$

$$Gl\mathbb{F}(2^2) = \frac{\mathbb{Z}_2[x]}{\left\langle x^2 + x + 1\right\rangle}$$

$$= \{a_0 + a_1x + \left\langle x^2 + x + 1\right\rangle \;\Big|\; a_0, \quad a_1 \in \mathbb{Z}_2, \quad i = 1, 2\}$$

$$\implies \quad Gl\mathbb{F}(2^2) = \{0+0.x+\left\langle x^2+x+1\right\rangle,\ 1+0.x+\left\langle x^2+x+1\right\rangle, 0+1.x+\left\langle x^2+x+1\right\rangle,\ 1+1.x+\left\langle x^2+x+1\right\rangle\}$$

$$\therefore \quad Gl\mathbb{F}(2^2) = \{0 + \left\langle x^2 + x + 1\right\rangle,\ 1 + \left\langle x^2 + x + 1\right\rangle,\ x + \left\langle x^2 + x + 1\right\rangle,\ 1 + x + \left\langle x^2 + x + 1\right\rangle\}$$

It is very simple to show $\{Gl\mathbb{F}(2^2), +\}$ is abelian group on mod 2 (Student must be show). so it is clearly

$$\{Gl\mathbb{F}(2^2),\ +\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

Now, For $\{Gl\mathbb{F}^*(2^2),\ .\}$ is group?

For this some operation be

$$x + \left\langle x^2 + x + 1\right\rangle, 1 + x + \left\langle x^2 + x + 1\right\rangle \in Gl\mathbb{F}(2^2)$$

Then

$$\left(x + \left\langle x^2 + x + 1\right\rangle\right)\left(1 + x + \left\langle x^2 + x + 1\right\rangle\right) = x + x^2 + \left\langle x^2 + x + 1\right\rangle$$

$$= -1 + \left\langle x^2 + x + 1\right\rangle \qquad \left(\textbf{Since} \;\; x^2 + x = -1\right)$$

$$= 1 + \left\langle x^2 + x + 1\right\rangle \in Gl\mathbb{F}(2^2) \qquad \left(\therefore \quad 1 = -\text{`1in} \;\; \mathbb{Z}_2\right)$$

Now,

$$\Big(1+x+\Big\langle x^2+x+1\Big\rangle\Big)\Big(1+x+\Big\langle x^2+x+1\Big\rangle\Big)=\Big(1+x\Big)^2+\Big\langle x^2+x+1\Big\rangle$$
$$=1+2x+x^2+\Big\langle x^2+x+1\Big\rangle$$
$$=x+\Big\langle x^2+x+1\Big\rangle\in Gl\mathbb{F}(2^2)\qquad\Big(Since\ \ 1+x+x^2=0\text{in}\ \ \mathbb{Z}_2\Big)$$

This type operation show that $1+\Big\langle x^2+x+1\Big\rangle$ is identity element in $Gl\mathbb{F}^*(2^2)$ under binary operation multiplication and their order is $\Big|1+\Big\langle x^2+x+1\Big\rangle\Big|=1$

Now order of elements in $Gl\mathbb{F}^*(2^2)$

$$\Big(1+x+\Big\langle x^2+x+1\Big\rangle\Big)^3=\Big(1+x+\Big\langle x^2+x+1\Big\rangle\Big(x+\Big\langle x^2+x+1\Big\rangle\Big)$$
$$=x+x^2+\Big\langle x^2+x+1\Big\rangle$$
$$=1+\Big\langle x^2+x+1\Big\rangle$$

$$\therefore\quad\Big|1+x+\Big\langle x^2+x+1\Big\rangle\Big|=3$$

Similarly, $\Big|x+\Big\langle x^2+x+1\Big\rangle\Big|=3.$

$$\therefore\quad Gl\mathbb{F}^*(2^2)\cong\mathbb{Z}_4^*\qquad\mathbb{Z}_4^*=\mathbb{Z}_4-\{0\}$$

Hence $\{Gl\mathbb{F}(2^2),\ +,\ .\}$ is field.

Assignment

Question:1. Construct Galois field of order 8 and 27.

Question:2. How many elements that satisfied $x^{26}=1$ in $Gl\mathbb{F}(3^5)$.

Question:3. Let $\mathbb{F}$ be finite field of order n $(=p^k, \text{for some}\ \ k)$ then $\forall\ \ 0\neq x\in\mathbb{F},\ \ x^{n-1}=1$.

Question:3. If $f(x)=x^2+2x-1\in\mathbb{F}_3[x]$ and $Gl\mathbb{F}(3^2)=\frac{\mathbb{F}_3[x]}{\Big\langle x^2+2x-1\Big\rangle}$, then which of the following is/are correct.

(a) $Gl\mathbb{F}(9)$ is field of order 9.
(b) $Aut\Big(Gl\mathbb{F}(3^2)-\{0\}\Big)$ is cyclic.
(c) $Aut\Big(Gl\mathbb{F}(3^2)-\{0\}\Big)$ is abelian but not cyclic.
(d) none

Ans. : a, c.

.....All the best.....