Subject : MATHEMATICS

Paper 1 : ABSTRACT ALGEBRA

Chapter 10 : Applications of Field Extensions

Module 2 : Characterizations of Galois fields

Anjan Kumar Bhuniya
Department of Mathematics
Visva-Bharati; Santiniketan
West Bengal

Characterizations of Galois fields

Learning Objectives:	1. Frobenius automorphism and its consequences.
	2. Subfields of a finite field.
	3. F is a finite field if and only if $(F^*, \cdot)$ is cyclic.
	4. Existence of an irreducible polynomial of degree n.

For every positive integer n and prime number p, there is a field of p^n elements. Also any two fields of p^n elements are isomorphic. We denote the field of order p^n by $GF(p^n)$.

For every prime number p and positive integer n, the field $GF(p^n)$ is the splitting field of $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Indeed every element of $GF(p^n)$ is a root of $f(x)$, that is

$$a^{p^n} = a, \qquad \text{for all } a \in GF(p^n).$$

This observation has far reaching consequences.

Theorem 0.1. *The mapping $\sigma : GF(p^n) \longrightarrow GF(p^n)$ defined by:*

$$\sigma(a) = a^p$$

is an automorphism.

Proof. Since p is prime, $p|{}^pc_r$ for all $0 < r < p$. Then $char\ F = p$ shows that ${}^pc_r a^{p-r}b^r = 0$ for all $0 < r < p$, and so $(a+b)^p = a^p + b^p$. Thus $\sigma(a+b) = \sigma(a) + \sigma(b)$. Also

$$\begin{aligned} \sigma(ab) &= (ab)^p \\ &= a^p b^p \\ &= \sigma(a)\sigma(b). \end{aligned}$$

Hence σ is a homomorphism.

Now let $b \in F$. Then $b = b^{p^n}$ implies that $b = \sigma(a)$ where $a = b^{p^{n-1}}$, and so σ is onto. Since F is finite, σ is also one-to-one. Thus σ is an automorphism. □

This automorphism σ is called the Frobenius automorphism.

Recall that a nonconstant polynomial $f(x) \in K[x]$ is said to be separable if roots of every irreducible factor of $f(x)$ in a splitting field are simple.

Corollary 0.2. *Every nonconstant polynomial over a finite field is separable.*

Proof. Let F be a finite field of p^n elements and $f(x)$ be an irreducible polynomial over F. If $f(x)$ is not separable then $f(x) = \sum_{i=1}^{r} a_i(x^p)^i$; $a_i \in F$. Then $a_i^{p^n} = a_i$ for all $i = 1, 2, \cdots, r$ implies that

$$f(x) = (\sum_{i=1}^{r} a_i^{p^{n-1}} x^i)^p$$

which contradicts that $f(x)$ is irreducible over F. Thus $f(x)$ and hence every polynomial over F is separable. □

Let F be a field of characteristic p. Denote $F^p = \{a^p \mid a \in F\}$. Then F is called perfect if $F^p = F$.

Corollary 0.3. *Every finite field is perfect.*

Proof. Let F be a finite field of characteristic p. Consider the Frobenius automorphism $\sigma : F \longrightarrow F$ defined by:

$$\sigma(a) = a^p$$

for all $a \in F$. Since σ is onto, $F = \sigma(F) = \{a^p \mid a \in F\} = F^p$. Thus F is perfect. □

Now we characterize subfields of $GF(p^n)$. If K is a subfield of $GF(p^n)$, then $(K, +)$ is a subgroup of $(GF(p^n), +)$ which implies, by the Lagrange's Theorem, that $|K| = p^m$ for some $0 \leq m < n$. Considering K as an intermediate field of $GF(p^n)/\mathbb{Z}_p$, tower rule gives us more specific characterization of the subfields of $GF(p^n)$.

Theorem 0.4. *For every positive integer $m \mid n$, $GF(p^n)$ has unique subfield $GF(p^m)$; and conversely every subfield of F is of the form $GF(p^m)$ for some $m \mid n$.*

Proof. If $m|n$, then $n = mk$ for some $k \in \mathbb{N}$. Then $p^n - 1 = (p^m)^k - 1 = (p^m - 1)(p^{m(k-1)} + \cdots + 1) = (p^m - 1)t$ where $t = p^{m(k-1)} + \cdots + 1$.

Hence

$$\begin{aligned} x^{p^n} - x &= x(x^{p^n - 1} - 1) \\ &= x(x^{(p^m-1)t} - 1) \\ &= x(x^{p^m-1} - 1)(x^{(p^m-1)(t-1)} + \cdots + 1) \\ &= (x^{p^m} - x)(x^{(p^m-1)(t-1)} + \cdots + 1) \end{aligned}$$

which implies that $x^{p^m} - x \mid x^{p^n} - x$.

Since $GF(p^n)$ is the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$, $x^{p^m} - x \mid x^{p^n} - x$ implies that $GF(p^n)$ contains the splitting field $GF(p^m)$ of $x^{p^m} - x$ over $\mathbb{Z}_p$.

The uniqueness follows from the fact that the polynomial $x^{p^m} - x$ can have at most p^m roots in F and every element of a field of order p^m is a root of the polynomial $x^{p^m} - x$.

Let K be a subfield of F. Then K is of characteristic p and so is an extension of $\mathbb{Z}_p$. Suppose $[K : \mathbb{Z}_p] = m$. Then $|K| = p^m$. Now the tower rule $[F : \mathbb{Z}_p] = [F : K][K : \mathbb{Z}_p]$ implies that $n = m[F : K]$. Thus $m \mid n$. □

Thus total number of subfields of $GF(p^n)$ is $\tau(n)$, the number of positive divisors of n.

Example 0.5. *Let F be a field of order 3^8. Then the above result shows that F has exactly as many subfields as the number of positive divisors of 8. Hence total number of subfields of F is 4.*

Since characteristic of $GF(p^n)$ is p, order of every nonzero element of $(GF(p^n), +)$ is p. Then it follows from the Fundamental Theorem of Finite Abelian Groups that $(GF(p^n), +)$ is the direct sum of n-copies of $\mathbb{Z}_p$. Now we show that the multiplicative group of $GF(p^n)$ is cyclic.

Theorem 0.6. *Let F be a field. Then $(F^*, \cdot)$ is cyclic if and only if F is a finite field.*

Proof. Assume that $F^* =< a >$ is cyclic. First we show that *char* $F \neq 0$. Otherwise, $-1 \neq 1$ which shows that $-1 = a^n$ and so $a^{2n} = 1$ for some positive integer n. Then $|F^*| = | < a > | = 0(a) \leq 2n$ implies that F is a finite field; which contradicts that F is of characteristic zero. Thus *char* $F \neq 0$. Let *char* $F = p$, p is a prime integer. Then F is an extension of $\mathbb{Z}_p$. This again implies that $F = \mathbb{Z}_p(a)$. Now we show that a is algebraic over $\mathbb{Z}_p$. If $a - 1 \neq 0, 1$, then $a - 1 = a^n$ for some $n \in \mathbb{N}$, which shows that a is a root of $x^n - x + 1 \in \mathbb{Z}_p[x]$. If $a - 1 = 0$ or $a - 1 = 1$, then $a = 1$ or $a = 2$ implies that $a \in \mathbb{Z}_p$. Thus in either case, a is algebraic over $\mathbb{Z}_p$ and so $[\mathbb{Z}_p(a) : \mathbb{Z}_p]$ is finite, say $[\mathbb{Z}_p(a) : \mathbb{Z}_p] = r$. Then $|F| = |\mathbb{Z}_p(a)| = p^r$. Hence F is a finite field.

Conversely assume that F is a finite field. Then F^* is a finite abelian group and so can be expressed as a direct sum $C_1 \oplus C_2 \oplus \cdots \oplus C_t$ of cyclic groups C_i such that $n_i \mid n_{i+1}$ for every $1 \leq i \leq t-1$ where $n_i = |C_i|$. It follows that $x^{n_t} = 1$ for every $x \in F^*$. Now the polynomial $x^{n_t} - 1$ of degree n_t can have at most n_t roots in the field F, and so $|F^*| \leq n_t$. Also $|F^*| \geq |C_t| = n_t$ which implies that $|F^*| = n_t$. Hence $F^* = C_t$ is a cyclic group. □

Now we give some interesting consequences of this result. Recall that an extension F/K is said to be simple if $F = K(c)$ for some $c \in F$. Now we show that $GF(p^n)$ is a simple extension of $\mathbb{Z}_p$.

Corollary 0.7. *Every finite extension of a finite field is a simple extension.*

Proof. Let F be a finite extension of a finite field K of characteristic p. Then F is a finite field and so $F^* =< c >$ for some $c \in F$. This implies that $F = \mathbb{Z}_p(c)$. Since $\mathbb{Z}_p \subseteq K \subseteq F$, it follows that $F = K(c)$. Thus F/K is a simple extension. □

Irreducibility of polynomials over a field is still as mysterious as the prime numbers. The following result can be treated as an analogue of the result that there are infinitely many primes numbers. The result shows that there are plenty of irreducible polynomials.

Corollary 0.8. *Let K be a finite field and d be a positive integer. Then there is an irreducible polynomial $p(x)$ of degree d over K.*

Proof. Let *char* $K = p$ and $|K| = p^m$. Denote $n = md$. Then there is a field F of order p^n. Since $m \mid n$, F has a subfield L of order p^m. Then K and L are isomorphic and hence F is an extension of K. Since F/K is a finite extension, it is simple, say $F = K(c)$ for some $c \in F$. Also F/K is an algebraic extension. Let $p(x) \in K[x]$ be the minimal polynomial of c over K. Then $p(x)$ is irreducible over K and $\deg p(x) = [K(c) : K] = [F : \mathbb{Z}_p]/[K : \mathbb{Z}_p] = \frac{n}{m} = d$ proves the result. □

Above result shows that there is an irreducible polynomial of degree n over $\mathbb{Z}_p$. Consider a field F of order p^n. Then $[F : \mathbb{Z}_p] = n$ and $F = \mathbb{Z}_p(c)$ for some $c \in F$. If $m(x) \in \mathbb{Z}_p[x]$ is the minimal polynomial of c over $\mathbb{Z}_p$, then $[\mathbb{Z}_p(c) : \mathbb{Z}_p] = n$ shows that $\deg m(x) = n$. Since c is a root of $x^{p^n} - x \in \mathbb{Z}_p[x]$, it follows that $m(x) \mid x^{p^n} - x$. This suggests us the following result:

Theorem 0.9. *The polynomial $x^{p^n} - x \in \mathbb{Z}_p[x]$ is precisely the product of all distinct irreducible polynomials over $\mathbb{Z}_p$ of degree d where d runs through all divisors of n.*

Consider $x^{2^2} - x$ over $\mathbb{Z}_2$. Then $x^4 - x$ is the product of all irreducible polynomials over $\mathbb{Z}_2$ of degree 1 and 2. Now x and $x - 1$ are the only irreducible polynomials of degree 1 over $\mathbb{Z}_2$ and so

$$\frac{x^4 - x}{x(x-1)} = x^2 + x + 1$$

is the only irreducible quadratic over $\mathbb{Z}_2$.

Consider $x^{2^3} - x$ over $\mathbb{Z}_2$ which is the product of all irreducible polynomials over $\mathbb{Z}_2$ of degree 1 and 3. Since x and $x - 1$ are the only irreducible polynomials of degree 1 over $\mathbb{Z}_2$,

$$\begin{aligned}\frac{x^8 - x}{x(x-1)} &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\ &= (x^3 + x^2 + 1)(x^3 + x + 1)\end{aligned}$$

shows that there are only two irreducible cubics over $\mathbb{Z}_2$, which are $x^3 + x^2 + 1$ and $x^3 + x + 1$.

1 Summary

- The mapping $\sigma : GF(p^n) \longrightarrow GF(p^n)$ defined by:

  $$\sigma(a) = a^p$$

  is an automorphism.

  This automorphism σ is called the Frobenius automorphism.

- Every nonconstant polynomial over a finite field is separable.
- Every finite field is perfect.
- For every positive integer $m \mid n$, $GF(p^n)$ has unique subfield $GF(p^m)$; and conversely every subfield of F is of the form $GF(p^m)$ for some $m \mid n$.
- Let F be a field. Then $(F^*, \cdot)$ is cyclic if and only if F is a finite field.
- Every finite extension of a finite field is a simple extension.
- Let K be a finite field and d be a positive integer. Then there is an irreducible polynomial $p(x)$ of degree d over K.
- For every prime number p and positive integer n, there is an irreducible polynomial $p(x)$ of degree n over $\mathbb{Z}_p$.
- The polynomial $x^{p^n} - x \in \mathbb{Z}_p[x]$ is precisely the product of all distinct irreducible polynomials over $\mathbb{Z}_p$ of degree d where d runs through all divisors of n.