Existence and Uniqueness of Galois fields

Learning Objectives:	1. Introduction to Galois fields.
	2. Order of a Galois field of characteristic p is p^n.
	3. For every prime p and $n \in \mathbb{N}$, there is a Galois field of order p^n.
	4. Any two Galois fields of order p^n are isomorphic.

A field F is called a Galois field if it contains finitely many elements. $\mathbb{Z}_2$, $\mathbb{Z}_3, \cdots$, in general $\mathbb{Z}_p$ for any prime number p are Galois fields. There are many other Galois fields. Since every Galois field is finite, they are of characteristic p for some prime number p. In this module we characterize all Galois fields of characteristic p as the splitting field of suitable polynomials over $\mathbb{Z}_p$. Galois fields containing same number of elements are isomorphic.

Every Galois field of characteristic p is an extension of $\mathbb{Z}_p$. As a consequence we have the following characterization on possible orders of a finite field.

Theorem 0.1. *Let F be a Galois field of characteristic p. Then $|F| = p^n$ for some positive integer n.*

Proof. Since F is of characteristic p, F is an extension of $\mathbb{Z}_p$; and since F is a finite field, $[F : \mathbb{Z}_p]$ is finite. Assume that $[F : \mathbb{Z}_p] = n$ and $\{e_1, e_2, \cdots, e_n\}$ is a basis of F as a vector space over $\mathbb{Z}_p$. Then every element $\alpha \in F$ can be expressed as

$$\alpha = c_1e_1 + c_2e_2 + \cdots + c_ne_n,$$

for some c_i in $\mathbb{Z}_p$, $i = 1, 2, \cdots, n$. Since such expressions are unique, F has as many elements as the total number of above expressions. Since each $c_i \in \mathbb{Z}_p$ can be chosen in p ways, total number of such expressions is p^n. □

Thus if n is a positive integer which has more than one prime factors, then there is no field containing n elements.

Example 0.2. *Is there any field of order 6?*

No, there is no field of order 6, since 6 is not a power of some prime.

Also we have following useful consequence.

Corollary 0.3. *Let F be a field. Then F is of characteristic p and $[F : \mathbb{Z}_p] = n$ if and only if $|F| = p^n$.*

Proof. Let F is of characteristic p and $[F : \mathbb{Z}_p] = n$. Then proceeding similarly as in the proof of the previous theorem, it follows that $|F| = p^n$.

Conversely, assume that $|F| = p^n$. Then F is a finite field and so *char* $F = q$ for some prime q. It follows that $o(1) = q$ in the group $(F, +)$ and hence $q \mid p^n$. Thus $q = p$ forcing characteristic of F to be p. So F is an extension of $\mathbb{Z}_p$ and finiteness of F implies that it is a finite extension of $\mathbb{Z}_p$. Let $[F : \mathbb{Z}_p] = m$. Then it follows from the first part that $|F| = p^m$. Hence $p^n = p^m$ which implies that $m = n$ and so $[F : \mathbb{Z}_p] = n$. □

Now we give an example of a Galois field other than the fields of the form $\mathbb{Z}_p$. If K is a field and $p(x)$ is an irreducible polynomial over K, then $F = K[x]/ < p(x) >$ is a field which is an extension of K and contains a root $\lambda = x + < p(x) >$ of $p(x)$. Hence $K(\lambda) \simeq K[x]/ < p(x) >$. If $\deg p(x) = n$, then $[K(\lambda) : K] = n$. Hence if we take $K = \mathbb{Z}_p$, then $K(\lambda)$ is a field of p^n elements. In the following, we construct a field of order $4 = 2^2$, for which we are to consider an irreducible polynomial of degree 2 over $\mathbb{Z}_2$.

Example 0.4. *Consider $\mathbb{Z}_2$ and an irreducible and monic polynomial $p(x) = x^2 + x + [1] \in \mathbb{Z}_2[x]$. Then $F = \mathbb{Z}_2[x]/ < x^2 + x + [1] >$ is a field which contains a root $\lambda = x + < x^2 + x + [1] >$ of $x^2 + x + [1]$. Thus $\lambda \in F$ is algebraic over $\mathbb{Z}_2$ with the minimal polynomial $x^2 + x + [1]$. Hence $\mathbb{Z}_2(\lambda) \simeq \mathbb{Z}_2[x]/ < x^2 + x + [1] >$ and so $F \simeq \mathbb{Z}_2(\lambda)$. We show that $\mathbb{Z}_2(\lambda)$ is a field of order 4. Since the degree of the minimal polynomial $x^2 + x + [1]$ of λ is 2, $\{[1], \lambda\}$ is a basis of $\mathbb{Z}_2(\lambda)/\mathbb{Z}_2$. Thus*

$$\mathbb{Z}_2(\lambda) = \{[0], [1], \lambda, [1] + \lambda\}.$$

The composition table for addition is given by:

$+$	$[0]$	$[1]$	λ	$[1] + \lambda$
$[0]$	$[0]$	$[1]$	λ	$[1] + \lambda$
$[1]$	$[1]$	$[0]$	$[1] + \lambda$	λ
λ	λ	$[1] + \lambda$	$[0]$	$[1]$
$[1] + \lambda$	$[1] + \lambda$	λ	$[1]$	$[0]$

The composition table for multiplication is given by:

$\cdot$	$[0]$	$[1]$	λ	$[1] + \lambda$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	λ	$[1] + \lambda$
λ	$[0]$	λ	$[1] + \lambda$	$[1]$
$[1] + \lambda$	$[0]$	$[1] + \lambda$	$[1]$	λ

In the previous theorem we have proved that order of every finite field is p^n for some prime number p and positive integer n. Now we show that the converse also holds.

Theorem 0.5. *For every prime integer p and $n \in \mathbb{N}$, there is a field of order p^n.*

Proof. Consider the field $\mathbb{Z}_p$ and the polynomial $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$. Let F be a splitting field of $f(x)$ over $\mathbb{Z}_p$. Then *char* $F = p$. First we show that the roots of $f(x)$ in F are distinct. Let $\alpha \in F$ be a root of $f(x)$ of order m. Then there is $g(x) \in F[x]$ such that $f(x) = (x-\alpha)^m g(x)$, and so $(x-\alpha)^m g(x) = x^{p^n} - x$ which implies that $m(x-\alpha)^{m-1}g(x) + (x-\alpha)^m g'(x) = -1$. Then $(x-\alpha)^{m-1} \mid -1$ shows that $m = 1$, and hence the roots of $f(x)$ in F are distinct.

Thus $L = \{\alpha \in F \mid f(\alpha) = 0\} = \{\alpha \in F \mid \alpha^{p^n} = \alpha\}$ contains exactly p^n elements. Now for $\alpha, \beta \in L$, $\beta \neq 0$, we have $(\alpha - \beta)^{p^n} = \alpha^{p^n} - \beta^{p^n} == \alpha - \beta$ and $(\alpha\beta^{-1})^{p^n} = \alpha^{p^n}(\beta^{p^n})^{-1} = \alpha\beta^{-1}$, and so $\alpha - \beta, \alpha\beta^{-1} \in L$. Hence L is a subfield of F. Thus L is a field of p^n elements. □

Note that, in the above proof, $L = F$.

Now we show that there is only one field of order p^n up to isomorphism.

Theorem 0.6. *Let F is a field of order p^n for some prime integer p and positive integer n. Then F is a splitting field of the polynomial $x^{p^n} - x$ over $\mathbb{Z}_p$.*

Proof. $(F^*, \cdot)$ is a group with identity 1. Then $|F^*| = p^n - 1$ and this implies that $c^{p^n - 1} = 1$, i.e. $c^{p^n} - c = 0$ for all $c \in F^*$. Thus every nonzero element of F is a root of the polynomial $x^{p^n} - x$ over $\mathbb{Z}_p$. 0 is also a root of this polynomial. Now a polynomial of degree p^n has exactly p^n roots in any of its splitting fields and F contains p^n elements each of which is a root of the polynomial $x^{p^n} - x$. Thus F is a splitting field of the polynomial $x^{p^n} - x$ over $\mathbb{Z}_p$. □

Given a polynomial $f(x)$ over a field K, any two splitting fields of $f(x)$ over K are isomorphic. This implies the following result.

Corollary 0.7. *Any two finite fields of the same order are isomorphic.*

1 Summary

- A field F is called a Galois field if it contains finitely many elements.
- Every Galois field is of characteristic p and so is an extension of $\mathbb{Z}_p$.
- Let F be a Galois field of characteristic p. Then $|F| = p^n$ for some positive integer n.
- If n is a positive integer which has more than one prime factors, then there is no field containing exactly n elements.
- Let F be a field. Then F is of characteristic p and $[F : \mathbb{Z}_p] = n$ if and only if $|F| = p^n$.
- If $p(x)$ is an irreducible polynomial over $\mathbb{Z}_p$ of degree n, then $\mathbb{Z}_p[x]/ < p(x) >$ is a field of p^n elements.

- For every prime integer p and $n \in \mathbb{N}$, there is a field of order p^n.
- Let F is a field of order p^n for some prime integer p and positive integer n. Then F is a splitting field of the polynomial $x^{p^n} - x$ over $\mathbb{Z}_p$.
- Any two finite fields of the same order are isomorphic.

epathshala पाठशाला A Gateway to All Post Graduate Courses