Fields and Galois Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

1 Finite Fields

Some Facts About Finite Fields

- A finite field K has characteristic p, a prime number.
- Its minimal subfield, known as its **prime subfield**, is

$$\{0_K, 1_K, 2(1_K), \ldots, (p-1)(1_K)\}.$$

- The prime subfield is isomorphic to $\mathbb{Z}_p$, the field of integers modulo p.
- For all x, y in a field K of characteristic p, and for all $n \geq 1$,

$$(x \pm y)^{p^n} = x^{p^n} \pm y^{p^n}.$$

The Formal Derivative

- Let
$$f = a_0 + a_1 X + \cdots + a_n X^n$$
be a polynomial with coefficients in a field K.
- The **formal derivative** Df of f is defined by
$$Df = a_1 + 2a_2 X + \cdots + na_n X^{n-1}.$$
- The familiar formulas from analysis hold.
For all $f, g \in K[X]$ and $k \in K$:
    - $D(kf) = k(Df)$;
    - $D(f+g) = Df + Dg$;
    - $D(fg) = (Df)g + f(Dg)$.

Roots of a Polynomial in a Splitting Field

Theorem

Let f be a polynomial with coefficients in a field K, and let L be a splitting field for f over K. Then the roots of f in L are all distinct if and only if f and Df have no non-constant common factor.

- Suppose first that f has a repeated root α in L.
  So we have $f = (X-\alpha)^r g$, where $r \geq 2$. Then
  $$Df = (X-\alpha)^r (Dg) + r(X-\alpha)^{r-1} g.$$
  So f and Df have the common factor $X-\alpha$.
  Conversely, suppose that f has no repeated roots.
  Then, for each root α of f in L, we have $f = (X-\alpha)g$, where $g(\alpha) \neq 0$.
  Hence, $Df = g + (X-\alpha)(Dg)$. So $(Df)(\alpha) = g(\alpha) \neq 0$.
  Thus, by the remainder theorem, $(X-\alpha) \nmid Df$.
  This holds for every factor of f in $L[X]$.
  So f and Df must be coprime.

Classification of Finite Fields

Theorem

(i) Let K be a finite field. Then $|K| = p^n$, for some prime p and some integer $n \geq 1$. Every element of K is a root of the polynomial $X^{p^n} - X$, and K is a splitting field of this polynomial over the prime subfield $\mathbb{Z}_p$.

(ii) Let p be a prime, and let $n \geq 1$ be an integer. There exists, up to isomorphism, exactly one field of order p^n.

(i) Let K have characteristic p. Then K is a finite extension of $\mathbb{Z}_p$, of degree n, say. Suppose $\{\delta_1, \delta_2, \ldots, \delta_n\}$ is a basis of K over $\mathbb{Z}_p$. Every element of K is uniquely expressible as a linear combination

$$a_1\delta_1 + a_2\delta_2 + \cdots + a_n\delta_n,$$

with coefficients in $\mathbb{Z}_p$. For each coefficient a_i there are p choices, namely $0, 1, \ldots, p-1$. So there are p^n linear combinations in all. Thus, $|K| = p^n$.

Classification of Finite Fields (Cont'd)

- The group K^* is of order $p^n - 1$. Let $\alpha \in K^*$. By Lagrange's theorem, the order of α, which is the order of the subgroup $\langle \alpha \rangle$ generated by α, divides $p^n - 1$. Certainly $\alpha^{p^n - 1} = 1$. Thus $\alpha^{p^n} - \alpha = 0$. But we also have $0^{p^n} - 0 = 0$. So every element of K is a root of $X^{p^n} - X$.

  Thus, $X - \alpha$ is a linear factor for each of the p^n elements α of K.

  It follows that the polynomial $X^{p^n} - X$ splits completely over K.

  It clearly cannot split completely over any proper subfield of K.

  So K must be the splitting field of $X^{p^n} - X$ over $\mathbb{Z}_p$.

Classification of Finite Fields (Part (ii))

(ii) Let p and n be given. Let L be the splitting field of $f = X^{p^n} - X$ over $\mathbb{Z}_p$. Since the field is of characteristic p, $Df = p^n X^{p^n - 1} - 1 = -1$. Thus, f and Df are coprime. So $X^{p^n} - X$ has p^n distinct roots in L.

Let K be the set of those roots. We show that K is a subfield of L. The elements $0, 1$ are clearly in K. Suppose that $a, b \in K$.

- $(a - b)^{p^n} = a^{p^n} - b^{p^n} = a - b$. So $a - b \in K$.
- If $b \neq 0$, $(ab^{-1})^{p^n} = a^{p^n}(b^{p^n})^{-1} = ab^{-1}$. So $ab^{-1} \in K$.

K contains (indeed consists of) all the roots of $X^{p^n} - X$. Clearly no proper subfield of K has this property. So K is the splitting field.

Thus, for all primes p and all integers $n \geq 1$, there exists a field of order p^n. Moreover, any field of order p^n is the splitting field of $X^{p^n} - X$ over $\mathbb{Z}_p$. We know all such fields are isomorphic.

- Only fields of prime-power order exist.
- Moreover, for a given p and n there is essentially exactly one field of order p^n, called the **Galois field of order p^n**, and denoted $\mathrm{GF}(p^n)$.

Group Theory: Order and Exponent

- Let G be a finite group.
- The **order** $o(a)$ of an element a in G is the least positive integer k, such that $a^k = 1$. We know $a^m = 1$ if and only if $o(a)$ divides m.
- The **exponent** $e = e(G)$ of G is the smallest positive integer $e = e(G)$ with the property that $a^e = 1$, for all a in G.
- The exponent always exists (in a finite group): It is the least common multiple of the orders of the elements of G.
- Since $o(a)$ divides $|G|$, for every a, we have $e(G)$ divides $|G|$.
- In a non-abelian group G it is possible that $o(a) < e(G)$, for all a in G.
  Consider the smallest non-abelian group $S_3 = \{1, a, b, x, y, z\}$ (table on the right).
  We have $o(1) = 1$, $o(x) = o(y) = o(z) = 2$, $o(a) = o(b) = 3$, and $e(S_3) = 6$.

	1	a	b	x	y	z
1	1	a	b	x	y	z
a	a	b	1	z	x	y
b	b	1	a	y	z	x
x	x	y	z	1	a	b
y	y	z	x	b	1	a
z	z	x	y	a	b	1

- This cannot happen, however, if the group is abelian.

The Exponent in the Abelian Case

Theorem

Let G be a finite abelian group with exponent e. Then there exists an element a in G, such that $o(a) = e$.

- Suppose that $e = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where:
  - $p_1, p_2, \ldots, p_k$ are distinct primes;
  - $\alpha_1, \alpha_2, \ldots, \alpha_k \geq 1$.

  e is the least common multiple of the orders of the elements of G.
  So there exists an element h_1 whose order is divisible by $p_1^{\alpha_1}$.
  Thus, $o(h_1) = p_1^{\alpha_1} q_1$, where q_1 divides $p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.
  Let $g_1 = h_1^{q_1}$. Then, for all $m \geq 1$, $g_1^m = h_1^{mq_1}$. And we have

  $$g_1^m = h_1^{mq_1} = 1 \quad \text{iff} \quad p_1^{\alpha_1} q_1 \mid mq_1 \quad \text{iff} \quad p_1^{\alpha_1} \mid m.$$

  Thus, $o(g_1) = p_1^{\alpha_1}$.
  Similarly, for $i = 2, \ldots, k$, we can find an element g_i of order $p_i^{\alpha_i}$.

The Exponent in the Abelian Case (Cont'd)

- We found, for $i = 1, 2, \ldots, k$, an element g_i of order $p_i^{\alpha_i}$.
  Let $a = g_1 g_2 \cdots g_k$, and let $n = o(a)$.
  Thus, $a^n = g_1^n g_2^n \cdots g_k^n = 1$ (using the abelian property).
  So $g_1^n = g_2^{-n} \cdots g_k^{-n}$.
  Let $r = p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.
  Now $o(g_i) = p_i^{\alpha_i}$. So $g_i^{-nr} = 1$, $i = 2, \ldots, k$. Hence, $g_1^{nr} = 1$.
  Thus, $p_1^{\alpha_1}$ divides nr. So, since p_1 and r are coprime, $p_1^{\alpha_1}$ divides n.
  Similarly, $p_i^{\alpha_i}$ divides n, for $i = 2, \ldots, k$. We deduce that $e \mid n$.
  By the definition of the exponent, $n \mid e$. Therefore, $o(a) = e$.

Corollary

If G is a finite abelian group such that $e(G) = |G|$, then G is cyclic.

Multiplicative Structure of GF(p^n)

Theorem

The group of non-zero elements of the Galois field GF(p^n) is cyclic.

- Denote GF(p^n) by K and, as usual, denote the abelian group of non-zero elements of K by K^*. Let e be the exponent of K^*.
  - Then $a^e = 1$, for all a in K^*. So every element of K^* is a root of the polynomial $X^e - 1$. This polynomial has at most e roots. So $|K^*| \leq e$.
  - But we also have $e \leq |K^*|$.

  Hence, $e = |K^*|$. So, by the corollary, K^* is cyclic.
- All fields of order p^n are isomorphic.

  So we can construct GF(p^n) by:
  - Finding an irreducible polynomial f of degree n in $\mathbb{Z}_p[X]$;
  - Taking $\text{GF}(p^n) = \mathbb{Z}_p[X]/\langle f \rangle$.

  There will, however, normally be may choices for f.

Example

- Recall that the non-zero elements of the field GF(9) are

$$1, -1, \alpha, 1+\alpha, -1+\alpha, -\alpha, 1-\alpha, -1-\alpha,$$

where $\alpha^2 = -1$.

The orders of the elements of the group are easily computed:

$$o(1) = 1,\ o(-1) = 2,\ o(\pm\alpha) = 4,\ o(\pm 1 \pm \alpha) = 8.$$

Any one of the four elements $\pm 1 \pm \alpha$ is a generator of the group.

E.g., the powers of $1+\alpha$ are

n	1	2	3	4	5	6	7	8
$(1+\alpha)^n$	$1+\alpha$	$-\alpha$	$1-\alpha$	-1	$-1-\alpha$	α	$-1+\alpha$	1