Chapter 5

Finite Fields

Many courses on Galois Theory finish with a final chapter which discusses the properties of finite fields and how the study of Galois Theory applies to them. In these lecture notes, however, I have chosen to place at this point in the notes the information about the structure of finite fields (in particular, their construction) since the methods developed in the previous two chapters are sufficient. It is also my plan to exploit the Theorem of the Primitive Element during our investigation of the main theory. This theorem essentially applies to infinite fields and consequently we need alternative methods for finite fields. Hence it will be important to establish that the multiplicative group of a finite field is cyclic, as we shall do in this chapter.

Construction of finite fields

Let F be a finite field. Then F has characteristic p for some prime number p and it has a subfield isomorphic to the finite field $\mathbb{F}_p$ (that is, the prime subfield of F). Let $n = |F : \mathbb{F}_p|$ be the degree of the extension. (As F is finite, it is certainly finite dimensional as a vector space over $\mathbb{F}_p$.) If $\{x_1, x_2, \dots, x_n\}$ is a basis for F over $\mathbb{F}_p$, then every element of F can be expressed uniquely in the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n$$

where $a_1, a_2, \dots, a_n \in \mathbb{F}_p$. Hence

$$|F| = p^n.$$

Thus, we can make our first observation:

Proposition 5.1 *A finite field F has order p^n where p is a prime number equal to the characteristic of F and where n is the degree of F over its prime subfield $\mathbb{F}_p$.* □

Note, in particular, this argument shows that a finite extension of the field $\mathbb{F}_p$ (or indeed of any finite field) is still a finite field.

Of course, Proposition 5.1 provides us with a restriction which finite fields could exists, namely that they must all have prime-power order, but we need to do more to show that fields of each such order do indeed exist. We shall need two observations in our argument.

Lemma 5.2 *Let F be a finite field of order $q = p^n$ and characteristic p. Then*

(i) $a^{q-1} = 1$ *for all $a \in F \setminus \{0\}$;*

(ii) ***("Freshman's Exponentiation")***

$$(a + b)^{p^k} = a^{p^k} + b^{p^k}$$

for all $a, b \in F$ and non-negative integers k.

Proof: (i) The set of non-zero elements of F forms the multiplicative group F^*, which is a group of order $q-1$, so $a^{q-1}=1$ for all $a \in F^*$ by Lagrange's Theorem.

(ii) We proceed by induction on k. When $k=0$, the result is immediate since both sides equal $a+b$. Now if $c, d \in F$, note that

$$(c+d)^p = \sum_{i=0}^{p} \binom{p}{i} c^i d^{p-i}. \tag{5.1}$$

We already observed (back in Example 1.24(iii)) that each binomial coefficient $\binom{p}{i}$ is divisible by p for $i = 1, 2, \dots, p-1$. Hence, in our field F of characteristic p,

$$(c+d)^p = c^p + d^p.$$

Returning to the inductive step,

$$\begin{aligned}
(a+b)^{p^{k+1}} &= \big((a+b)^{p^k}\big)^p \\
&= (a^{p^k} + b^{p^k})^p && \text{by induction} \\
&= (a^{p^k})^p + (b^{p^k})^p && \text{by Equation (5.1)} \\
&= a^{p^{k+1}} + b^{p^{k+1}},
\end{aligned}$$

completing the induction. □

We can now establish that there exists a finite field of each prime-power order and, moreover, it is unique.

Theorem 5.3 *Let p be a prime number and n be a positive integer. Then there is precisely one field of order p^n up to isomorphism.*

Proof: We start by establishing existence. Let $f(X) = X^{p^n} - X$ and let F be the splitting field of $f(X)$ over $\mathbb{F}_p$ (which exists by Theorem 3.4). Let S be the set of roots of $f(X)$ in F. Note certainly $0, 1 \in S$. If $a, b \in S$, then $a^{p^n} = a$, $b^{p^n} = b$, so

$$\begin{aligned}
(ab)^{p^n} &= a^{p^n} b^{p^n} = ab \\
(a+b)^{p^n} &= a^{p^n} + b^{p^n} = a+b \\
(-a)^{p^n} &= (-1)^{p^n} a^{p^n} = -a \\
(1/a)^{p^n} &= 1/a^{p^n} = 1/a
\end{aligned}$$

(if $a \neq 0$ in the last). Note here that in the second equation we use Freshman's Exponentiation (Lemma 5.2(ii)), while in the third note that $(-1)^{p^n} = -1$ when p is odd, while $(-1)^{p^n} = 1 = -1$ when $p=2$. The conclusion is that S is a subfield of F. In particular, S must contain the prime subfield, so $\mathbb{F}_p \subseteq S$. However, we now recall that F is the splitting field of $f(X)$ over $\mathbb{F}_p$ and so is the smallest field containing $\mathbb{F}_p$ and all the roots of $f(X)$; that is, $F = S$, so we record:

Every element of F is a root of $f(X)$.

To determine the order of the splitting field F, we shall determine the number of roots of $f(X)$ in F. Observe the formal derivative of $f(X)$ is

$$Df(X) = p^n X^{p^n - 1} - 1 = -1$$

and we conclude that $f(X)$ and $Df(X)$ have no common factor of degree one or more. Hence, by Lemma 4.5, the polynomial $f(X)$ has no repeated roots in the splitting field F; that is, $f(X)$ has precisely p^n roots in F. We conclude:

$$\text{The splitting field } F \text{ is a finite field of order } p^n.$$

To establish uniqueness, consider any field K of order p^n, so that K is an extension of the prime subfield $\mathbb{F}_p$ of degree n. The multiplicative group of K has order $p^n - 1$, so

$$a^{p^n-1} = 1 \qquad \text{for all } a \in K \setminus \{0\}$$

and therefore

$$a^{p^n} = a \qquad \text{for all } a \in K.$$

We conclude that our polynomial $f(X)$ has p^n distinct roots in K and therefore this polynomial splits in K; that is, K is a splitting field for $f(X)$ over $\mathbb{F}_p$. We now use the fact that splitting fields are unique (Corollary 3.8) to conclude that K is $\mathbb{F}_p$-isomorphic to the field F constructed previously. This completes the proof. □

Definition 5.4 The (unique) field of order p^n is denoted $\mathbb{F}_{p^n}$ and is often called the *Galois field* of order p^n.

Although the theorem establishes that the Galois field $\mathbb{F}_{p^n}$ is the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$, this is not necessarily a convenient description to construct the field. It is often easier to go back to Theorem 2.13 which describes how to construct a simple extension with a specified minimum polynomial.

Example 5.5 Construct the Galois field $\mathbb{F}_4$ of order 4 and give its multiplication table.

Solution: Let $f(X) = X^2 + X + 1$ over $\mathbb{F}_2$. Note that this polynomial is irreducible over $\mathbb{F}_2$ since

$$f(0) = f(1) = 1$$

so $f(X)$ has no linear factors. Adjoin a root α of $f(X)$ over $\mathbb{F}_2$ to construct the simple extension $\mathbb{F}_2(\alpha)$. Thus we have a degree 2 extension of $\mathbb{F}_2$ with basis $\{1, \alpha\}$. The elements of $\mathbb{F}_2(\alpha)$ are

$$0, \quad 1, \quad \alpha, \quad \alpha + 1$$

so $\mathbb{F}_2(\alpha) \cong \mathbb{F}_4$ (using the uniqueness of finite fields that we have established in Theorem 5.3). Addition is straightforward: we just use the vector space structure. The multiplication is achieved by exploiting the fact that $f(\alpha) = 0$, so $\alpha^2 = \alpha + 1$. Hence the multiplication table of $\mathbb{F}_4$ is:

	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Indeed, observe for example

$$\alpha(\alpha + 1) = \alpha^2 + \alpha = 1.$$

□

The multiplicative group of a finite field

In this section, we shall show that the mutliplicative group of a finite field is always a cyclic group. In some examples that we know, this can be seen straightaway. For example, $\mathbb{F}_4^*$ is a group of order 3, so is cyclic generated by any non-identity element and indeed, in the notation of the solution for Example 5.5,

$$\alpha, \qquad \alpha^2 = \alpha + 1, \qquad \alpha^3 = \alpha^2 + \alpha = 1$$

are the three non-zero elements of $\mathbb{F}^4$. Equally, if we calculate the powers of 3 in $\mathbb{F}^7$, we observe they are

$$3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1.$$

This example does illustrate the need for care though, since 3 is a generator for $\mathbb{F}_7^*$, but 2 does not generate this multiplicative group.

To work towards showing that the multiplicative group of a finite field is indeed cyclic, we begin by introducing the following terminology:

Definition 5.6 The *exponent* of a finite group is the least common multiple of the orders of elements of G.

Note that Lagrange's Theorem tells us that the order of every element of a finite group G divides the order of G and hence the exponent of G also divides $|G|$.

Lemma 5.7 *Let G be a finite abelian group with exponent ν. Then there exists some $g \in G$ of order ν.*

This could be established relatively quickly from the Classification of Finite Abelian Groups as direct products of cyclic groups. The proof presented here will be direct without requiring explicit use of that result. (Some aspects of the proof will be in common with the proof of said Classification.)

PROOF: First factorize ν into its product of primes,

$$\nu = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

and let $q = p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Consider an element $x_1 \in G$ such that the order of x is a power of p_1 and that $o(x_1) = p_1^{\beta}$ with β as large as possible.

Claim: $\beta = \alpha_1$.

Since ν is the lowest common multiple of the element orders, certainly p_1^{β} divides ν and so $\beta \leqslant \alpha_1$. Suppose $\beta < \alpha_1$. Then if $h \in G$, we note, from the fact that $o(h)$ divides ν, that

$$1 = h^{\nu} = (h^q)^{p_1^{\alpha_1}},$$

so h^q is an element of p_1-power order. From our assumption on x as having the largest p_1-power order in G, we conclude then that $(h^q)^{p_1^{\beta}} = 1$; that is,

$$h^{p_1^{\beta} q} = 1$$

so the order of h divides $p_1^{\beta} q$. This is true for all elements h in G and we conclude that the lowest common multiple of the orders of elements in G divides

$$p_1^{\beta} q = p_1^{\beta} p_2^{\alpha_2} \dots p_k^{\alpha_k} < \nu,$$

contrary to the assumption that ν is the exponent of G.

In conclusion, $\beta = \alpha_1$ and we observe that there is an element x_1 in G of order $p_1^{\alpha_1}$.

Similarly, we now conclude that there are elements $x_1, x_2, \dots, x_k$ in G with $o(x_i) = p_i^{\alpha_i}$. Finally, as $x_1, x_2, \dots, x_k$ commute and have coprime orders, we conclude

$$o(x_1 x_2 \dots x_k) = o(x_1)\, o(x_2) \dots o(x_k) = \nu,$$

as required. □

Theorem 5.8 *The multiplicative group of a finite field is cyclic.*

PROOF: Let F be a finite field of order p^n. Let ν be the exponent of the multiplicative group. Since ν is divisible by the order of any element $a \in F^*$, we conclude

$$a^\nu = 1 \qquad \text{for all } a \in F \setminus \{0\}.$$

Hence

$$a^{\nu+1} - a = 0 \qquad \text{for all } a \in F.$$

We conclude that the polynomial $X^{\nu+1} - X$ has p^n roots in F, so its degree $\nu + 1 \geqslant p^n$. On the other hand, we know that the exponent ν divides the group order $|F^*|$ by Lagrange's Theorem (as noted before), so $\nu \leqslant p^n - 1$. We conclude therefore that

$$\nu = p^n - 1.$$

Now Lemma 5.7 tells us that F^* contains an element g of order $p^n - 1$, so $F^* = \langle g \rangle$, as required. □

We can use the fact that the multiplicative group is cyclic to provide an alternative to the Theorem of the Primitive Element for finite fields.

Corollary 5.9 *Let $F \subseteq K$ be an extension of finite fields. Then $K = F(\alpha)$ for some $\alpha \in K$.*

PROOF: Indeed, choose α to be the generator for K^*. Then the smallest subfield containing α must be the whole of K, so $K = F(\alpha)$. □

Putting Theorem 4.11 together with Corollary 5.9, we conclude that if K is a finite separable extension of F, then $K = F(\alpha)$ for some $\alpha \in K$ irrespective of whether F is an infinite field or a finite field.