Galois Theory - Week 10 - Finite Fields

Antonio León Villares

June 2022

Contents

Based on the notes by Tom Leinster, Chapter 10

1 Classifying Finite Fields

1.1 Lemma: Order of Finite Fields

> *Let M be a **finite** field. Then:*
>
> 1. *char$(M) = p$, where p is **prime***
> 2. *$|M| = P^n$, where $n = [M : \mathbb{F}_p] \geq 1$*
>
> *(Lemma 10.1.1)*

Proof. Claim (1) is the statement of Lemma 2.3.17. For (2), since M is finite, its prime subfield is $\mathbb{F}_p$ (by Lemma 2.3.16). Let $1 \leq n < \infty$ be such that $n = [M : \mathbb{F}_p]$. Then, M is an n-dimensional vector space over $\mathbb{F}_p$, so in particular it is isomorphic to $\mathbb{F}_p^n$, so:

$$|M| = |\mathbb{F}_p^n| = |\mathbb{F}_p|^n = p^n$$

as required. □

1.2 Finite Fields Have Prime Power Order

1.2.1 Lemma: Existence of Prime Power Order Fields

> *Let p be **prime** and $n \geq 1$. Then, the **splitting field** of:*
>
> $$f = t^{p^n} - t \in \mathbb{F}_p[t]$$
>
> *has order p^n.*
> *(Lemma 10.1.5)*

Proof. Let $M = SF_{\mathbb{F}_{|}}(f)$. We need to show that $|M| = p^n$.

On the one hand, we compute:

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

by using the fact that $\mathbb{F}_p$ has characteristic p. Now, recall:

> *Let f be a non-zero polynomial over a* ***field*** *K. The following are* ***equivalent****:*
>
> 1. *f has a* ***repeated root*** *in $SF_K(f)$*
> 2. *f and Df have a* ***common root*** *in $SF_K(f)$*
> 3. *f and Df have a* ***non-constant common factor*** *in $K[t]$*
>
> *(Lemma 7.2.9)*

In particular, since f and Df have no common roots, it must be the case that f has no repeated roots in M, so all of these roots must be in M, and so, $|M| \geq p^n$.

On the other hand, let θ be the Frobenius map of M, such that if $\alpha \in M$, $\theta(\alpha) = \alpha^p$. Then:

$$\theta^n(\alpha) = \alpha^{p^n}$$

Now, let L be the set of roots of f in M. Then:

$$\alpha \in L \iff \alpha^{p^n} = \alpha \iff \theta^n(\alpha) = \alpha$$

Hence,

$$L = Fix\{\theta^n\}$$

θ is a homomorphism, so by

> *Let M be a* ***field****. Denote with $Aut(M)$ the* ***group*** *of* ***automorphisms*** *of M. Then:*
>
> $$\forall S \subseteq Aut(M),\ Fix(S) \text{ is a } \textbf{subfield} \text{ of } M$$
>
> *We call $Fix(S)$ the* ***fixed field*** *of S.*
> *(Lemma 7.3.1)*

we have that L is a subfield of M. But then, L is a subfield of M containing the roots of f, and where f splits, so by definition, $L = M$. Thus, every element of M must be a root of f. Since $\deg(f) = p^n$, f has at most p^n roots, so $|M| \leq p^n$.

All in all, it thus follows that $|M| = p^n$, as required.

□

1.2.2 Lemma: Uniqueness of Prime Power Order Fields

> *Every* ***finite*** *field of order ‖ is a* ***splitting field*** *of $t^q - t$ over $\mathbb{F}_p$.*
> *(Lemma 10.1.8)*

Proof. We begin by showing that if $|M| = q$, then:

$$\forall \alpha \in M, \alpha^q = \alpha$$

This is essentially Fermat's Little Theorem adapted outside of the modulo p world. The multiplicative group $M^\times$ has order $q - 1$, so by Lagrange's Theorem:

$$\forall \alpha \in M^\times, \alpha^{q-1} = 1_M$$

so in particular, if $0_M \neq \alpha \in M$:

$$\alpha^q = \alpha$$

If $\alpha = 0_M$, the equation holds.

Now, let $|M| = q$. By lemma 10.1.1 above, we must have that:

$$\exists p, n \geq 1 : q = p^n \wedge char(M) = p$$

where p is prime. Thus, M has $\mathbb{F}_p$ as a prime subfield. By what we have just shown above, every element of M must be a root of:

$$f(t) = t^q - t = t^{p^n} - t$$

Thus, M is generated by the set of roots of f (since M **is** the set of roots of f). Moreover, since f has $|M| = p^n = \deg(f)$ distinct roots in M, clearly f must split in M. Thus, M is a splitting field of f. □

1.2.3 Theorem: Classification of Finite Fields

1. *Every* ***finite*** *field has order p^n, for some* ***prime*** *p and integer $n \geq 1$.*
2. *For each prime p and integer $n \geq 1$, there is a* ***unique*** *field of order p^n (up to ismorphism). It has* ***characteristic*** *p, and it is the* ***splitting field*** *of $t^{p^n} - t$ over $\mathbb{F}_p$.*

(Theorem 10.1.9)

Proof. This follows immediately from all of the results above, alongside the uniqueness of splitting fields. □

2 Multiplicative Structure of Finite Fields

2.1 Proposition: Cyclic Subgroups from Group of Units

Let K be a ***field****. Then, every* ***finite subgroup*** *of $K^\times$ is cyclic. In particular, if K is* ***finite****, then $K^\times$ is cyclic.*
(Proposition 10.2.1)

Proof. This is a result from the Group Theory course (Theorem 5.1.13, Corollary 5.1.14; see my notes), requiring the use of group exponents/Fundamental Theorem of Finite Abelian Groups. □

2.2 Example: Generalising Roots of Unity

- when working over fields like $\mathbb{C}$, we know that the nth root of unity is $\omega = e^{2\pi i/n}$
- ω is useful, in the sense that any other root of $t^n - 1$ is just a power of ω
- if we want to generalise this to an arbitrary field K, define:

  $$U_n(K) = \{\alpha \in K \mid \alpha^n = 1_K\}$$

  Then, $U_n(K)$ is a multiplicative subgroup of K, so in particular it is a multiplicative subgroup of $K^\times$, so $U_n(K)$ must be cyclic
- we can define ω to be the **generator** of $U_n(K)$, and then if $\alpha \in U_n(K)$, then $\exists k : \omega^k = \alpha$, so the nth roots of unity in K will be powers of ω
- however, unlike with the standard case, $U_n(K)$ need not have n elements; that is, $o(\omega) \leq n$
- for example, if $char(K) = p$, then $U_p(K) = \{1_K\}$.

2.3 Corolla: Extensions of Finite Fields are Simple

*Every **extension** of a **finite** field over another field is **simple**.*
(Corollary 10.2.5)

Proof. Let $M : K$ be an extension with M finite. The group $M^\times$ is cyclic, so:

$$\exists \alpha \in M^\times \ : \ M^\times = \langle a \rangle$$

Hence, $M = K(\alpha)$, since $0_K \in K \implies 0_K \in M$. □

2.4 Corollary: Existence of Irreducible Polynomials of Given Degree

*Let p be **prime**, and $n \geq 1$ an integer. Then, there exists an **irreducible** polynomial over $\mathbb{F}_p$ of degree n.*
(Corollary 10.2.8)

This is quite non-trivial. For example, it shows that there are irreducible polynomials of degree 23, 100 and 32897402813 over $\mathbb{F}_{31}$.

Proof. The prime subfield of $\mathbb{F}_{p^n}$ is $\mathbb{F}_p$. Then, by the above corollary, $\mathbb{F}_{p^n} : \mathbb{F}_p$ must be a simple extension, say $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$. Then, the minimal polynomial of α over $\mathbb{F}_p$ is irreducible, and has degree:

$$[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$$

□

3 Galois Groups for Finite Fields

3.1 Lemma: Fundamental Theorem in Finite Fields

*Let $M : K$ be a **field extension**.*

1. *If K is **finite**, then $M : K$ is **separable**.*
2. *If M is also **finite**, then $M : K$ is **finite** and **normal**.*

(Lemma 10.3.2)

Proof. (1)

Let $f \in K[t]$ be irreducible, where $p = char(K) > 0$. Suppose for contradiction that f is inseparable. By

*Let K be a **field**. Then:*

1. *If $char(K) = 0$, then every **irreducible** polynomial over K is **separable**.*
2. *If $char(K) = p > 0$, then for an **irreducible** polynomial $f \in K[t]$:*

$$f \text{ is } \textbf{\textit{inseparable}} \iff f(t) = \sum_{i=0}^{r} b_i t^{ip}$$

where $b_0, \ldots, b_r \in K$.

(Corollary 7.2.11)

it follows that:

$$f(t) = \sum_i b_i t^{pi}, \qquad b_i \in K$$

Moreover, by

> *Let p be a **prime**:*
>
> 1. *In a **field** of **characteristic** p, every element has **at most one** pth root*
> 2. *In a **finite field** of **characteristic** p, every element has **exactly one** pth root*
>
> *(Corollary 2.3.22)*

each b_i has exactly one root; that is:

$$\forall b_i, \exists c_i \in K \; : \; b_i = c_i^p$$

Hence, we can write:

$$f(t) = \sum_i c_i^p t^{pi} = \sum_i (c_i t^i)^p$$

But then, using the fact that the Frobenius Map $a \mapsto a^p$ is a homomorphism:

$$f(t) = \left(\sum_i (_i t^i \right)^p$$

so f can't be irreducible. Hence, we have a contradiction, and f must be separable. Hence, every irreducible polynomial in $M : K$ is separable, so it is a separable extension.

(2)

Now, that M is finite and $chat(M) = p > 0$. By Theorem 10.1.9 above, M is a splitting field over $\mathbb{F}_p$. In particular, by

1. *Let:*

   - $M : S : K$ *be a* ***field extension***
   - $$0_K \neq f \in K[t]$$
   - $Y \subseteq M$

   Let S *be the* ***splitting field*** *of* f *over* K*. Then,* $S(Y)$ *is the* ***splitting field*** *of* f *over* $K(Y)$*:*

   $$S = SF_K(f) \implies S(Y) = SF_{K(Y)}(f)$$

2. *Let:*

   - $$0_K \neq f \in K[t]$$
   - L *be a* ***subfield*** *of* $SF_K(f)$ *containing* K*, such that:*

     $$SF_K(f) : L : K$$

   Then, $SF_K(f)$ *is the* ***splitting field*** *of* f *over* L*:*

   $$SF_K(f) = SF_L(f)$$

(Lemma 6.2.14)

M is also a splitting field over K. Hence, by

Let $M : K$ *be a* ***field extension****. Then, for some non-zero* $f \in K[t]$*:*

$$M = SF_K(f) \iff M : K \text{ is } \textbf{finite} \text{ and } \textbf{normal}$$

(Theorem 7.1.5)

$M : K$ is finite and normal.

□

3.2 The Galois Correspondence for Finite Fields

3.2.1 Proposition: Galois Group is Cyclic

*Let p be a prime and $n \geq 1$. Then, $Gal(\mathbb{F}_{p^n} : \mathbb{F}_p)$ is **cyclic** of order n, and is generated by the **Frobenius automorphisms** of $\mathbb{F}_{p^n}$.*
(Proposition 10.3.3)

Proof. Let θ be the Frobenius automorphism of $\mathbb{F}_{p^n}$, such that if $\alpha \in \mathbb{F}_{p^n}$, then $\theta(\alpha) = \alpha^p$. Now, from the proof of Lemma 10.1.8 above, if M is a finite field of order q, then $\forall \alpha \in M, \alpha^q = \alpha$. In particular, if $\alpha \in \mathbb{F}_p$, then $\theta(\alpha) = \alpha$, so θ is an automorphism of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, so $\theta \in Gal(\mathbb{F}_{p^n} : \mathbb{F}_p)$. Moreover,

$$\forall \alpha \in \mathbb{F}_{p^n}, \alpha^{p^n} = \alpha \implies \theta^n(\alpha) = \alpha$$

Now, assume $\exists m \in \mathbb{Z}$ such that $\theta^m = \text{id}$. Then, $\alpha^{p^m} = \alpha$ for any $\alpha \in \mathbb{F}_{p^n}$. Thus, any $\alpha \in \mathbb{F}_{p^n}$ satisfies the polynomial $t^{p^m} - t$. Hence, the number of roots of $t^{p^m} - t$ in $\mathbb{F}_{p^n}$ is at least p^n; since it has degree p^m, it must then be the case that $p^n \leq p^m \iff n \leq m$. Hence, θ must have order n.

But now, by the Fundamental Theorem of Galois Theory:

$$|Gal(\mathbb{F}_{p^n} : \mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$$

Hence, $Gal(\mathbb{F}_{p^n} : \mathbb{F}_p)$ is a group of order n, and θ has order n, so it must be a cyclic group generated by θ, as required.

□

3.2.2 Proposition: Subfields of Galois Group

*Let p be a **prime** and $n \geq 1$. Then, $\mathbb{F}_{p^n}$ has a **unique** subfield of order p^m, for each **divisor** m of n, and no others. In particular, this subfield is:*

$$\left\{\alpha \in \mathbb{F}_{p^n} \;\middle|\; \alpha^{p^m} = \alpha\right\}$$

(Proposition 10.3.6)

---

*Notice, this requires that $m|n$, **not** that $m \leq n$. For instance, $\mathbb{F}_8$ has no subfield isomorphic to $\mathbb{F}_4$, since $8 = 2^3$ and $4 = 2^2$, but $2 \nmid 3$.*

Proof. Let $G = Gal(\mathbb{F}_{p^n} : \mathbb{F}_p)$. By the Fundamental Theorem of Galois Theory, the intermediate fields of $\mathbb{F}_{p^n} : \mathbb{F}_p$ are in a one-to-one correspondence with the subgroups H fo G. Since G is cyclic generated by the Frobenius automorphism, any such H is of the form:

$$H = \left\langle \theta^{n/k} \right\rangle$$

where $k \mid n$ (any subgroup must have order dividing n, and any subgroup must be cyclic and thus generated by some power of θ). Then, the intermediate fields are precisely the fixed fields $Fix(H)$. Thus:

$$Fix \left\langle \theta^{n/k} \right\rangle = \left\{ \alpha \in \mathbb{F}_{p^n} \;\middle|\; \alpha^{p^{n/k}} = \alpha \right\}$$

Then, by the Tower Law alongsid ethe fundamental Theorem gives that:

$$|Fix \left\langle \theta^{n/k} \right\rangle| = [Fix \left\langle \theta^{n/k} \right\rangle : \mathbb{F}_p] = \frac{[\mathbb{F}_{p^n} : \mathbb{F}_p]}{[\mathbb{F}_{p^n} : Fix \left\langle \theta^{n/k} \right\rangle]} = \frac{n}{| \left\langle \theta^{n/k} \right\rangle |} = \frac{n}{k}$$

so in particular, $|Fix \left\langle \theta^{n/k} \right\rangle| = \frac{n}{k}$. Calling $m = \frac{n}{k}$, it follows that m is a divisor of n, as required.

□

3.2.3 Proposition: Galois Group of any Finite Field Extensions

The above propositions have worried about Galois Groups of field extensions where the base field was $\mathbb{F}_p$. We now generalise to arbitrary fields.

> *Let $M : K$ be a* ***field extension*** *with M* ***finite****. Then, $Gal(M : K)$ is* ***cyclic*** *and has order $[M : K]$.*
> *(Proposition 10.3.8)*

Proof. Since M is finite, it is isomorphic to $\mathbb{F}_{p^n}$, for some prime p and integer $n \geq 1$. By Proposition 10.3.6 above, M has exactly one subfield isomorphic to $\mathbb{F}_{p^m}$. Without ambiguity, we must have that K is isomorphic to one such $\mathbb{F}_{p^m}$.

Since $\mathbb{F}_{p^m} = Fix \langle \theta^m \rangle$ and $\langle \theta^m \rangle \cong C_{n/m}$, by the Fundamental Theorem of Galois Theory:

$$Gal(\mathbb{F}_{p^n} : Fix \langle \theta^m \rangle) = \langle \theta^m \rangle \implies Gal(\mathbb{F}_{p^n} : \mathbb{F}_{p^m}) \cong \mathbb{C}_{n/m}$$

That $n/m = [M : K]$ follows by the Tower Law.

□

3.2.4 Corollary: Quotients of Cyclic Groups

> *Let $m|n$. Then:*
> $$\frac{C_n}{C_{n/m}} \cong C_m$$

Proof. In the Galois Correspondence of $\mathbb{F}_{p^n} : \mathbb{F}_p$, all extensions and subgroups involed are normal (since cyclic groups are abelian). Hence, we have that:

$$\frac{Gal(\mathbb{F}_{p^n} : \mathbb{F}_p)}{Gal(\mathbb{F}_{p^n} : \mathbb{F}_{p^m})} \cong Gal(\mathbb{F}_{p^m} : \mathbb{F}_p)$$

But this is equivalent to:

$$\frac{C_n}{C_{n/m}} \cong C_m$$

as required. Alternatively, substituting $k = n/m$:

$$\frac{C_n}{C_k} \cong C_{n/k}$$

□

3.2.5 Example: Computing Galois Correspondence

The Galois Correspondence for $\mathbb{F}_{p^{12}} : \mathbb{F}_p$ for **any** prime p is given by: