Summary of results: Fields and Galois Theory

Alan Haynes, haynes@math.uh.edu

Last update: January 31, 2022

1. Field extensions

If K and F are fields with $F \subseteq K$ then we say that K is a **field extension** of F (or just an **extension** of F). We write K/F to refer to this field extension. If K is an extension of F then it is naturally an F-vector space, and we define the **degree** of K/F by

$$[K : F] = \dim_F(K).$$

If $[K : F] < \infty$ then we say that K/F is a **finite extension**. The following basic result should be familiar from linear algebra.

Theorem 1 (Tower Law)**.** *Suppose F, K, and L are fields satisfying the inclusions $F \subseteq K \subseteq L$. Then we have that:*

(i) $[L : F] = [L : K] \cdot [K : F]$.

(ii) If $\mathcal{A}$ is an F-basis for K/F and if $\mathcal{B}$ is a K-basis for L/K then the set

$$\mathcal{C} = \{\alpha\beta : \alpha \in \mathcal{A}, \beta \in \mathcal{B}\}$$

is an F-basis for L/F.

Suppose K/F and L/K are field extensions with $[K : F] = m$ and $[L : K] = n$, and that $\{\alpha_1, \ldots \alpha_m\}$ is an F-basis for K, and $\{\beta_1, \ldots, \beta_n\}$ is a K-basis for L. Then it follows from the Tower Law that $[L : F] = mn$ and that the set

$$\{\alpha_i\beta_j : 1 \leq i \leq m, 1 \leq j \leq n\}$$

is an F-basis for L/K. In other words, every element of L can be written uniquely in the form

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}\alpha_i\beta_j,$$

with coefficients a_{ij} taken from F.

The **characteristic** of F, denoted $\mathrm{char}(F)$, is the smallest positive integer n with the property that $na = 0$ for all $a \in F$, if such an integer exists. If no such integer exists then $\mathrm{char}(F) = 0$. We leave it to the reader to check that if $\mathrm{char}(F)$ is not 0 then it must be a prime number. Every field F contains a unique smallest subfield, called the

prime subfield of F. The prime subfield of F is isomorphic either to $\mathbb{Q}$ (if $\text{char}(F) = 0$) or to $\mathbb{F}_p$, for some prime p (if $\text{char}(F) = p$).

If K/F is an extension and $\mathcal{A} \subseteq K$, then the **field obtained from F by adjoining $\boldsymbol{\mathcal{A}}$**, denoted by $F(\mathcal{A})$, is the smallest subfield of K containing $F \cup \mathcal{A}$. If there exists an element $\alpha \in K$ such that $K = F(\alpha)$ then we say that K/F is a **simple extension**. If K/F is a field extension and if $\alpha, \beta \in K$, then $F(\alpha, \beta) = F(\alpha)(\beta)$.

Next, suppose that $F_1, \ldots, F_\ell$ are subfields of a common field K. The **composite extension** (or **compositum**) of $F_1, \ldots, F_\ell$ is defined to be the smallest subfield of K which contains all of them. It is denoted by $F_1 F_2 \cdots F_\ell$. The following result is useful in many problems.

Lemma 1. *Suppose that F_1 and F_2 are finite extensions of a common base field F. Then there is an extension K of F which contains F_1 and F_2. Furthermore, if $\{\alpha_1, \ldots, \alpha_n\}$ is an F-basis for F_1/F and $\{\beta_1, \ldots, \beta_m\}$ is an F-basis for F_2/F then:*

(i) $F_1 F_2 = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$.
(ii) $F_1 F_2$ *is the F-linear span of the set*

$$\{\alpha_i \beta_j : 1 \leq i \leq n, 1 \leq j \leq m\}.$$

(iii) $[F_1 F_2 : F] \leq [F_1 : F] \cdot [F_2 : F]$.

Although this result is similar in spirit to the Tower Law, be careful to understand the difference in setup: the result in the lemma is about composite extensions, not towers of extensions. In particular, note that part (iii) of the lemma here only provides an inequality. Nevertheless, this can be useful in practice.

2. Algebraic extensions

In many problems we will want to move from some field F to an extension field K in which a given polynomial in $F[x]$ has a root. For this the following result is foundational.

Theorem 2 (Kronecker's Theorem)**.** *If F is a field and $f \in F[x]$ is a nonconstant polynomial, then there is an extension of F in which f has a root.*

Corollary 1. *If F is a field and $f \in F[x]$ is a nonconstant polynomial, then there in an extension of F in which f* ***splits completely*** *(i.e. factors as a product of linear polynomials).*

If F is a field and $f \in F[x]$ is a nonconstant polynomial then there is a smallest extension field of F in which f splits completely, and it is unique up to isomorphism. This field is called the **splitting field of f over F**. If K is the splitting field of a degree n polynomial in $F[x]$ then $[K : F] \leq n!$.

The following result, which can be viewed as a more detailed version of Kronecker's Theorem, is also crucial to understanding field extensions obtained by adjoining roots of polynomials.

Theorem 3. *Suppose that F is a field and that $f \in F[x]$ is an irreducible polynomial. Let $\deg(f) = n$ and let α be a root of f in some extension of F. Then we have that:*

(i) The field $F(\alpha)$ is field isomorphic to $F[x]/(f(x))$, and an explicit isomorphism is given by the map $\alpha \mapsto x + (f(x))$.

(ii) $[F(\alpha) : F] = n$, and the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is an F-basis for $F(\alpha)$ as an F-vector space. In other words, every element of $F(\alpha)$ has a unique representation of the form

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1},$$

with coefficients $a_0, \ldots, a_{n-1}$ taken from F.

If K/F is a field extension then an element $\alpha \in K$ is **algebraic** over F if it is the root of a polynomial in $F[x]$. In this case then the **minimal polynomial for α over F**, denoted by f_α, is defined to be the unique monic irreducible polynomial in $F[x]$ which has α as a root. Note that the definition of f_α depends not only on α, but also on the field F. It follows from the above theorem that, if α is algebraic over F, then

$$[F(\alpha) : F] = \deg(f_\alpha).$$

The field K is said to be algebraic over F (and K/F is called an **algebraic extension**) if every element of K is algebraic over F. Note that if $[K : F] < \infty$ then K/F is an algebraic extension, but the converse of this statement is not true in general.

A field K is called **algebraically closed** if every polynomial in $K[x]$ splits completely in K. It is a non-trivial fact that every field F has an algebraic extension which is also algebraically closed, and that up to isomorphism there is only one such extension of F. This algebraically closed algebraic extension of F is called the **algebraic closure** of F, and it is denoted by $\overline{F}$.

A polynomial $f \in F[x]$ is **separable** if it has no repeated roots in $\overline{F}$. Otherwise f is **inseparable**. An extension K/F is **separable** if every $\alpha \in K$ is the root of a separable poynomial in $F[x]$. Otherwise the extension is **inseparable**. It is clear any separable extension must be algebraic. The following result is extremely useful.

Theorem 4 (Primitive Element Theorem)**.** *If K/F is a separable extension and $[K : F] < \infty$ then K/F is a simple extension.*

From this it is not difficult to deduce the following result.

Corollary 2. *Suppose that K/F is a field extension with $[K : F] < \infty$. If $\mathrm{char}(F) = 0$ or if $|F| < \infty$ then K/F is a simple extension.*

Finally, if K and L are fields an **embedding** of K into L is an injective field homomorphism from K into L. We have the following result about embeddings of separable field extensions into algebraic closures.

Theorem 5. *Suppose that K/F is a separable extension with $[K : F] = n$, write $K = F(\alpha)$, and let $\alpha_1, \ldots, \alpha_n$ be the distinct roots of f_α (the* ***conjugates*** *of α) in $\overline{F}$. Then there are exactly n distinct embeddings of K into $\overline{F}$ which fix F, and they are determined uniquely by the maps $\alpha \mapsto \alpha_i$, for $1 \leq i \leq n$.*

3. Finite fields

There are several basic but important facts about finite fields which you should know. We state these as theorems below, and we also include proofs that we hope will help to reinforce some of the information presented thus far.

Theorem 6. *If F is a field and $|F| < \infty$ then $|F| = p^n$, for some prime number p and for some $n \in \mathbb{N}$.*

Proof. If F is a finite field then its prime subfield must be $\mathbb{F}_p$, for some prime p. Then, if $[F : \mathbb{F}_p] = n$, we have that $|F| = |\mathbb{F}_p|^n = p^n$. □

Theorem 7. *For every prime p and for every $n \in \mathbb{N}$, there is exactly one finite field of order p^n, up to isomorphism.*

Proof. First we show that, for each prime p and $n \in \mathbb{N}$, there is a field of order p^n. Let K be the splitting field over $\mathbb{F}_p$ of the polynomial

$$f(x) = x^{p^n} - x \in \mathbb{F}_p[x].$$

Note that $[K : F] \leq (p^n)!$, which implies that K is finite. Since $f'(x) = -1$ in $\mathbb{F}_p[x]$, the polynomial f is separable (any repeated root of f in $\overline{\mathbb{F}_p}$

would also be a root f'). Therefore all the roots of f in K are distinct, showing that $|K| \geq p^n$. On the other hand, if α and β are roots of f then we have that

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta,$$

and (using the Binomial Theorem and the fact that we are working in characteristic p)

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta.$$

This shows that $\alpha\beta$ and $\alpha + \beta$ are also roots of F. Since the collection of roots of f is a finite subset of the finite field K which is closed under addition and multiplication, it is itself a field. Therefore, by the definition of the splitting field, it must equal K. This shows that $|K| = p^n$.

Next, suppose that L is any field of order p^n. Then L contains $\mathbb{F}_p$ as its prime subfield. By Fermat's Theorem, for any $\alpha \in L$, we have that

$$\alpha^{|L|} = \alpha^{p^n} = \alpha.$$

This shows that L is the splitting field over $\mathbb{F}_p$ of the polynomial f defined above. It follows from the uniqueness of the splitting field that L is isomorphic to the field K constructed above. □

Next we would like establish that the multiplicative group of any finite field is a cyclic group. In fact the following slightly more general result is true.

Theorem 8. *Suppose that F is any field. Any finite subgroup of the multiplicative group $F^\times$ is cyclic.*

Proof. Let G be a finite subgroup of $F^\times$. By the Fundamental Theorem of Finite Abelian Groups, there are integers $k \in \mathbb{N}$ and $n_1, n_2, \ldots, n_k \geq 2$ satisfying $n_i | n_{i+1}$ for each $1 \leq i < k$ and

$$G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k},$$

where each $\mathbb{Z}_{n_i}$ is a cyclic group of order n_i. Let $f \in F[x]$ be the polynomial

$$f(x) = x^{n_k} - 1.$$

The order of every element of G divides n_k, so every element of G is a root of f. Since F is a field, the polynomial f can have at most $\deg(f) = n_k$ roots in F. This forces $k = 1$, which means that G is a cyclic group. □

As a corollary of the previous theorem we immediately obtain the following result.

Corollary 3. *If F is a finite field then the multiplicative group $F^\times = F \setminus \{0\}$ is a cyclic group.*

4. Galois Theory

If K is a field then an isomorphism from K to itself is called an **automorphism** of K. The collection of all automorphisms of K is denoted by $\mathrm{Aut}(K)$. An element $\sigma \in \mathrm{Aut}(K)$ **fixes** a subset $A \subseteq K$ if $\sigma a = a$ for every $a \in A$. If K/F is a field extension the the collection of automorphisms of K which fix F is denoted $\mathrm{Aut}(K/F)$.

The set $\mathrm{Aut}(K)$ forms a group under composition of maps, and $\mathrm{Aut}(K/F)$ forms a subgroup. For any subgroup $H \leqslant \mathrm{Aut}(K)$, the collection of elements fixed by H, denoted K_H, is a subfield of K, called the **fixed field** of H.

Suppose that K/F is a field extension and that $\alpha \in K$ is algebraic over F. Let f_α be the minimal polynomial for α over F. Then it is an important fact (which you should know how to prove) that, for any $\sigma \in \mathrm{Aut}(K/F)$, we have that $f_\alpha(\sigma(\alpha)) = 0$. This shows that elements of $\mathrm{Aut}(K/F)$ permute the roots of f_α.

In trying to understand the group $\mathrm{Aut}(K/F)$, it is often useful to combine the above observation with the following fact: If K/F is given by $K = F(\alpha_1, \ldots, \alpha_n)$, then every element $\sigma \in \mathrm{Aut}(K/F)$ is uniquely determined by the values of $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$. This shows, in particular, that if K/F is a finite extension then $|\mathrm{Aut}(K/F)| < \infty$. In fact, we can say more.

Theorem 9. *If K/F is any finite extension then*

$$|\mathrm{Aut}(K/F)| \leq [K : F],$$

with equality if and only if F is the fixed field of $\mathrm{Aut}(K/F)$.

A finite extension K/F is called a **Galois extension** if $|\mathrm{Aut}(K/F)|$ is equal to $[K : F]$. In this case, $\mathrm{Aut}(K/F)$ is also called the **Galois group** of K/F, and denoted by $\mathrm{Gal}(K/F)$. The theorem above gives one characterization of Galois extensions. Another characterization is the following.

Theorem 10. *A finite extension K/F is Galois if and only if K is the splitting field of a separable polynomial with coefficients in F. Furthermore, if K/F is Galois then it is separable and every irreducible polynomial in $F[x]$ which has a root in K, splits completely.*

If K/F is a Galois extension then for any $\alpha \in K$ the elements $\sigma(\alpha)$, with $\sigma \in \mathrm{Gal}(K/F)$, are called the **Galois conjugates** (or just **conjugates**) of α. One important fact is that, if $K = F(\alpha)$ then all of the roots of f_α are Galois conjugates. This is also often phrased as saying that the Galois group acts transitively on the roots of f_α.

We conclude with one of the most beautiful theorems in this subject, which provides an explicit bijection between subgroups of the Galois group of a Galois extension, and intermediate fields of the extension.

Theorem 11 (**Fundamental Theorem of Galois Theory**). *If K/F is a Galois extension, with Galois group G, then:*

(i) *There is a bijection between subgroups H of G and intermediate fields of the extension K/F, given by the map $H \mapsto K_H$. Furthermore, $[K : K_H] = |H|$ (equivalently, $[K_H : F] = |G : H|$).*

(ii) *For each $H \leqslant G$, the extension K_H/F is Galois if and only if H is normal in G. If K_H/F is Galois then $\mathrm{Gal}(K_H/F) \cong G/H$.*