Fields and Galois Theory

Rachel Epstein

September 12, 2006

All proofs are omitted here. They may be found in Fraleigh's *A First Course in Abstract Algebra* as well as many other algebra and Galois theory texts. Many of the proofs are short, and can be done as exercises.

1 Introduction

Definition 1. A **field** is a commutative ring with identity, such that every non-zero element has a multiplicative inverse. That is, a field is a commutative division ring.

Some people prefer to think of fields in terms of the field axioms:

1. Addition is commutative: $a + b = b + a$
2. Addition is associative: $(a + b) + c = a + (b + c)$
3. There is an additive identity 0: $0 + a = a = a + 0$
4. Every element has an additive inverse: $a + (-a) = 0 = (-a) + a$
5. Multiplication is associative: $(ab)c = a(bc)$
6. Multiplication is commutative: $ab = ba$
7. There is a multiplicative identity 1: $1a = a = a1$
8. Every non-zero element has a multiplicative inverse: $a(a^{-1}) = 1 = (a^{-1})a$
9. The distributive law holds: a(b+c)=ab+ac

Definition 2. A field E is an **extension field** of a field F if $F \leq E$.

2 Conjugate Elements

Definition 3. Let $F[x]$ be the ring of polynomials with coefficients in F. A polynomial $p(x) \in F[x]$ is **irreducible over** F if it cannot be expressed as the product of two polynomials in $F[x]$ of strictly lower degree.

Example 4. $x^2 - 2$ is irreducible over $\mathbf{Q}$.
$x^2 + 1$ is irreducible over $\mathbf{R}$.
$x^2 - 1$ is reducible over $\mathbf{Q}$.

Definition 5. Let $F \leq E$, let $\alpha \in E$ be algebraic over F. Then the **irreducible polynomial of** α **over** F, $\mathrm{irr}(\alpha, F)$, is the unique monic polynomial $p(x)$ such that $p(x)$ is irreducible over F and $p(\alpha) = 0$.

Example 6. The irreducible polynomial of $\sqrt{2} \in \mathbf{R}$ over $\mathbf{Q}$ is $x^2 - 2$.

Definition 7. Let $F \leq E$. Two elements $\alpha, \beta \in E$ are **conjugate over** F if they have the same irreducible polynomial over F.

Example 8. In $\mathbf{C}$, some conjugates over $\mathbf{Q}$ are:

$$i,\ -i,\ p(x) = x^2 + 1$$
$$\sqrt{2},\ -\sqrt{2},\ p(x) = x^2 - 2$$
$$2^{1/3},\ 2^{1/3}e^{2\pi i/3},\ 2^{1/3}e^{4\pi i/3},\ p(x) = x^3 - 2$$

Theorem 2.1. *If α is algebraic over F, with irr(α, F) having degree $n \geq 1$, then the smallest field containing α and F, denoted $F(\alpha)$, consists exactly of elements of the form*

$$\gamma = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1},\ b_i \in F.$$

Theorem 2.2. *Let α, β be algebraic over F. Then the map $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ given by*

$$\psi_{\alpha,\beta}(b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}) = b_0 + b_1\beta + \cdots + b_{n-1}\beta^{n-1}$$

is an isomorphism if and only if α and β are conjugate.

Example 9. $\psi_{\sqrt{2},\sqrt{3}} : \mathbf{Q}(\sqrt{2}) \to \mathbf{Q}(\sqrt{3})$ is not an isomorphism since $\sqrt{2}$ is not conjugate to $\sqrt{3}$ over $\mathbf{Q}$.
$\mathbf{Q}(2^{1/3}) \simeq \mathbf{Q}(2^{1/3}e^{2\pi i/3})$ via the irreducible polynomial $x^3 - 2$.

3 Finite Extensions and Isomorphisms

Definition 10. If E is an extension field of F, then E is a vector space over F. If it has finite dimension n as a vector space over F, then E is a **finite extension of degree** n **over** F. We denote the degree of E over F as $[E : F]$.

Example 11. $\mathbf{C}$ is a 2-dimensional vector space over $\mathbf{R}$, so $[\mathbf{C} : \mathbf{R}] = 2$.
$\mathbf{Q}(\sqrt{2}, \sqrt{3})$, the smallest field containing $\mathbf{Q}$, $\sqrt{2}$, and $\sqrt{3}$, is generated by $\{1, \sqrt{3}\}$ over $\mathbf{Q}(\sqrt{2})$. $\mathbf{Q}(\sqrt{2})$ is generated by $\{1, \sqrt{2}\}$ over $\mathbf{Q}$. So we can see that $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is generated by $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ over $\mathbf{Q}$, and $[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}] = 4$.

Definition 12. An isomorphism of a field onto itself is called an **automorphism** of the field.

Definition 13. Let σ be an isomorphism of E on to some field, and let $\alpha \in E$ and $F \leq E$. Then σ **fixes** α if $\sigma(\alpha) = \alpha$, and σ **fixes** F if σ fixes each element in F.

Theorem 3.1. *Let $F \leq E$, and let σ be an automorphism of E leaving F fixed. Let $\alpha \in E$. Then $\sigma(\alpha) = \beta$ where β is a conjugate of α over F.*

Theorem 3.2. *Let $F \leq E$. The set $G(E/F)$of all automorphisms of E leaving F fixed forms a subgroup of the group of all automorphisms of E. We call $G(E/F)$the* **group of E over F**.

Theorem 3.3. *Let E_σ be the subset of E left fixed by an automorphism σ. Then E_σ is a field. We call this the* **fixed field of** *σ. Similarly, if S is a subgroup of $G(E/F)$, then the set E_S is a subfield of E.*

Theorem 3.4 (Isomorphism Extension Theorem)**.** *Let σ be an isomorphism from a field F to a field F', and let $\bar{F'}$ be an algebraic closure of F'. Let $F \leq E$. Then there exists at least one isomorphism τ of E onto a subfield $\bar{F'}$ such that for all $\alpha \in F$, $\tau(\alpha) = \sigma(\alpha)$.*

Theorem 3.5. *Let E be a finite extension of F. Let $\sigma : F \longrightarrow F'$ be an isomorphism. The number of extensions of σ to an isomorphism τ of E onto a subfield of $\bar{F'}$ is finite and depends only on E and F, not on σ or F'. We call this number $\{E : F\}$, the* **index of E over F**.

Theorem 3.6. *If E is a finite extension of F, then $\{E : F\}$ divides $[E : F]$.*

Definition 14. E is a **separable extension of** F if $\{E : F\} = [E : F]$. A field F is **perfect** if every finite extension of F is separable.

Perfect fields are in fact commonplace.

Theorem 3.7. *Every field of characteristic 0 is perfect. Every finite field is perfect.*

Definition 15. Let $\{p_i(x) : i \in I\}$ be a collection of polynomials in $F[x]$. Then $E \leq \bar{F}$ is the **splitting field** of $\{p_i(x) : i \in I\}$ over F if E is the smallest subfield of $\bar{F}$ containing F and all the zeros of each $p_i(x)$ in $\bar{F}$.

Example 16. $\mathbf{Q}(\sqrt{2},\sqrt{3})$ is the splitting field of $\{x^2-2, x^2-3\}$, and also of $\{x^4-5x^2+6\}$.

$\mathbf{Q}(2^{1/3})$ is not a splitting field because it does not contain the other two roots of x^3-2, which is irreducible.

Theorem 3.8. *Let $F \leq E \leq \bar{F}$. Then E be a splitting field over F if and only if every automorphism of $\bar{F}$ leaving F fixed maps E onto itself.*

Corollary 3.9. *If $E \leq \bar{F}$ and E is a splitting field over F of finite degree, then $\{E : F\} = |G(E/F)|$.*

Theorem 3.10 (Primitive Element Theorem)**.** *Let E be a finite separable extension of a field F. Then there exists $\alpha \in E$ such that $E = F(\alpha)$.*

Theorem 3.11. *If E is a finite extension of F and is a separable splitting field over F, then $|G(E/F)| = \{E : F\} = [E : F]$.*

Definition 17. A finite extension K of F is a **finite normal extension** of F if K is a separable splitting field over F. In such a case, we call G$(K/F)$the **Galois group of K over F.**

4 Fundamental Theorem of Galois Theory

Theorem 4.1 (Fundamental Theorem of Galois Theory)**.** *Let K be a finite normal extension of F. For all E such that $F \leq E \leq K$, let $\lambda(E) =$G(K/E). Then λ is a one-to-one map from the set of all intermediate fields onto the set of subgroups of G(K/F). The following properties hold:*

1. *$E = K_{G(K/E)} = K_{\lambda(E)}$. This is just saying that the field fixed by the set of automorphisms of K that fix E is E.*

2. *For $S \leq$G(K/F), $\lambda(K_S) = S$. That is, G$(K/K_S) = S$, or the set of automorphisms fixing the field fixed by S, is S.*

3. *$[K : E] = |G(K/E)|$, and $[E : F] = (G(K/F){:}G(K/E))$.*

4. *E is a normal extension of F if and only if G$(K/E)$is a normal subgroup of G(K/F). If so, then G$(E/F) \simeq$G$(K/F)/$G(K/E).*

5. *The diagram of subgroups of G$(K/F)$is the inverted diagram of the intermediate fields between F and K.*

Example 18. Let $K = \mathbf{Q}(\sqrt{2},\sqrt{3})$, and let $F = \mathbf{Q}$. Then each automorphism of K is determined by where it takes $\sqrt{2}$ and $\sqrt{3}$. Since each automorphism must take elements to their conjugates, the automorphisms are:

$$i(\sqrt{2}) = \sqrt{2}, i(\sqrt{3}) = \sqrt{3}$$
$$\sigma_1(\sqrt{2}) = -\sqrt{2}, \sigma_1(\sqrt{3}) = \sqrt{3}$$
$$\sigma_2(\sqrt{2}) = \sqrt{2}, \sigma_2(\sqrt{3}) = -\sqrt{3}$$
$$\sigma_3(\sqrt{2}) = -\sqrt{2}, \sigma_3(\sqrt{3}) = -\sqrt{3}$$

Here are the subgroup and intermediate field diagrams: