Last Revised: December 7, 2001

Lecture Notes on Fields (Fall 1997)

By George F. Seelinger

NOTE: All references here are either made to Hungerford or to Beachy/Blair (2nd Edition). The references to Hungerford start with roman numerals while the references to Beachy/Blair are of the form $x.y.z$ for positive integers x, y, and z. All internal references will be of the form $x.y$ for positive integers x and y.

1 Field Extensions

Definition 1.1 *Let F be a field and let $K \subseteq F$ be a subring. Then we say K is a subfield of F if K is a field. In this case we also call F an* **extension field** *of K and abbreviate this by saying F/K is a* **field extension**.

Recall the definition of a vector space over an arbitrary field.

Definition 1.2 *A* **vector space** *over a field K is an abelian group V whose group operation is denoted additively such that there exists a function $* : K \times V \to V$ with the following properties:*

1. *$(ab) * x = a * (b * x)$ for all $a, b \in K$ and $x \in V$.*
2. *$(a + b) * x = a * x + b * x$ for all $a, b \in K$ and $x \in V$.*
3. *$a * (x + y) = a * x + a * y$ for all $a \in K$ and $x, y \in V$.*
4. *$1 * x = x$ for all $x \in V$*

Then the following lemma tells us we can use some of the tools of linear algebra to help us study field extensions.

Lemma 1.3 *If F/K is a field extension, then F is a K vector space.*

Proof: By definition, F is an abelian group under addition, so we can define our vector addition to be the addition in F. Also, we can define our scalar multiplication $* : K \times F \to F$ to be given by $k * x = kx$ where the second multiplication is just multiplication of elements in F. Then it is easy to check that F satisfies the definition of a vector space with scalars K with these operations. Q.E.D.

So if F/K is a field extension, we define $[F:K] = \dim_K(F)$, the dimension of F as a K vector space. Therefore, $[F:K]$ is the cardinality of any basis of F as a K-vector space.

Review: Let V be a K-vector space for some field K. Let B be a non-empty subset of V. Then the **K-span** of B is the set of all *finite* sums of the form

$$a_1v_1 + \cdots + a_nv_n \quad \text{such that } a_1, \ldots, a_n \in K \text{ and } v_1, \ldots, v_n \in B$$

We say that B is **linearly independent over** K if for any $n \in \mathbb{N}$ and for any $v_1, \ldots, v_n \in B$ the only solution $a_1, \ldots, a_n \in K$ to the equation

$$a_1v_1 + \ldots + a_nv_n = 0$$

is the trivial one, $a_1 = a_2 = \cdots = a_n = 0$. Then a **$K$-basis** of V is a subset $B \subseteq V$ such that the K-span of B is V and B is linearly independent over K.

Now let F/K be a field extension and choose $u \in F$. Then we can define $K(u)$ to be the smallest subfield of F containing K and u. Hence for any subfield E of F such that $K \subseteq E$ and $u \in E$ we have $K(u) \subseteq E$. We call the extension $K(u)/K$ a **simple extension**. We can build more complicated extensions by taking a finite list of elements $u_1, \ldots, u_n \in F$ and defining $K(u_1, \ldots, u_n)$ to be the smallest subfield of F containing the set $\{u_1, \ldots, u_n\}$ and K. In general, for any subset $X \subseteq F$, we define $K(X)$ to be the smallest subfield of F containing K and X.

First we try to understand simple extensions. Let F/K be a field extension and choose $u \in F$. Then there exists an **evaluation homomorphism** $\phi_u : K[x] \to F$ given by $\phi_u(\sum_{i=0}^n a_i x^i) = \sum_{i=0}^n a_i u^i$ for every $n \in \mathbb{N}$ and every $a_0, \ldots, a_n \in K$. (It is not hard to see that ϕ_u is a homomorphism if you note $\phi_u(p) = p(u)$ for every $p \in K[x]$.) Furthermore, it is straightforward to see that $\mathrm{Im}\phi_\mathrm{u} \subseteq \mathrm{K(u)}$ since $K(u)$ is closed under addition and multiplication.

Definition 1.4 *Let F/K be a field extension. Then an element $u \in F$ is said to be* **algebraic over** *K if there exists a non-zero $p \in K[x]$ such that $p(u) = 0$. (This is equivalent to saying $\ker(\phi_u) \neq 0$.) We say that u is* **transcendental over** *K if it is not algebraic over K. (Hence u is transcendental over K if $\ker(\phi_u) = 0$.) We say that F is* **algebraic over** *K if every element of F is algebraic over K. If F is not algebraic over K, we say F is* **transcendental** *over K.*

Theorem 1.6 *Let F/K be a field extension and let $u \in F$.*

1. *If u is transcendental over K then $K(u) \cong K(x)$.*
2. *If u is algebraic over K then $K(u) \cong K[x]/\langle p \rangle$ for some irreducible $p \in K[x]$. Also $n = [K(u):K] = \deg(\mathrm{p})$ and $\{1, u, u^2, \ldots, u^{n-1}\}$ is a basis for $K(u)$.*

PROOF: (1) Assume u is transcendental over K. Then for every nonzero $g \in K[x]$ we have $g(u) = \phi_u(g) \neq 0$ must be an invertible element of $K(u)$, hence for any $f, g \in K[x]$ with $g \neq 0$ we have $f(u)/g(u) \in K(u)$. Therefore we can define a homomorphism $\tilde{\phi}_u : K(x) \to K(u)$ given by $\tilde{\phi}_u(f/g) = f(u)/g(u)$ for all $f/g \in K(x)$. As $\tilde{\phi}_u$ is non-trivial, it must be a monomorphism. Therefore $\mathrm{Im}\tilde{\phi}_\mathrm{u}$ is a subfield of $K(u)$ containing both u and K, hence must be equal to $K(u)$. So our result follows from the first isomorphism theorem.

(2) Assume u is algebraic over K. Then $\ker(\phi_u) = \langle p \rangle$ for some nonzero $p \in K[x]$. We claim that p must be irreducible, hence $\langle p \rangle$ is a maximal ideal of $K[x]$. Indeed, if $fg = p$ for some $f, g \in K[x]$ of strictly lower degree, then $f(u)g(u) = p(u) = 0$. As F is a field we have $f(u) = 0$ or $g(u) = 0$, which gives us $f \in \ker(\phi_u)$ or $g \in \ker(\phi_u)$. Therefore $f = pq$ or $g = pq$ for some $q \in K[x]$. This is a contradiction, hence p must be irreducible.

Now since p is irreducible, $\mathrm{Im}(\phi_\mathrm{u}) \cong \mathrm{K[x]}/\langle \mathrm{p} \rangle$ is a field that contains K and u, hence we have $\mathrm{Im}(\phi_\mathrm{u}) \subseteq \mathrm{K(u)} \subseteq \mathrm{Im}(\phi_\mathrm{u})$, so the first isomorphism theorem gives us that $K(u) \cong K[x]/\langle p \rangle$ as required.

Next we show that $U = \{1, u, u^2, \ldots, u^{n-1}\}$ is a basis of $K(u)$ over K, where $n = \deg(\mathrm{p})$. For any $w \in K(u)$ there exists an $f \in K[x]$ such that $\phi_u(f) = w$. By the Division Algorithm, $f = pq + r$ for some $q, r \in K[x]$ such that $r = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ for some $a_0, \ldots, a_{n-1} \in K$. As $pq \in \ker(\phi_u)$, we have $w = \phi_u(f) = \phi_u(r) = a_0 1 + a_1 u + \cdots + a_{n-1}u^{n-1}$. Therefore U spans $K(u)$. Also, if $a_0 1 + a_1 u + \cdots + a_{n-1}u^{n-1} = 0$ for some $a_0, \ldots, a_{n-1} \in K$, then $\sum_{i=0}^{n-1} a_i x^i \in \ker(\phi_u)$. As this has degree smaller than p, we must have $\sum_{i=0}^{n-1} a_i x^i = 0$. Therefore we have that $a_i = 0$ for all $0 \leq i \leq n-1$, so U is also linearly independent, hence a basis for $K(u)$. Q.E.D.

If F/K is an extension and $u \in F$ is algebraic over K then we define the **minimal polynomial of** u to be the unique monic irreducible polynomial $p \in K[x]$ such that $p(u) = 0$. Note that the minimal polynomial of u is also the unique monic generator of $\ker(\phi_u)$ where ϕ_u is the evaluation homomorphism. We define the **degree of** u **over** K to be the degree of the minimal polynomial of u.

One important observation to make from this theorem is that if $u \in F$ is algebraic over a subfield K of degree n then every element $c \in K(u)$ can be written uniquely in the form

$$c = a_0 + a_1 u + \cdots + a_{n-1}u^{n-1}$$

for some $a_0, \ldots, a_{n-1} \in K$.

Example: If we consider $F = \mathbb{Q}(\sqrt[3]{2})$ then since $x^3 - 2$ is irreducible over $\mathbb{Q}$, by Theorem 1.6 the set $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ is a $\mathbb{Q}$-basis of F, hence every element of $v \in F$ can be written uniquely as $v = a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}$ for some $a_0, a_1, a_2 \in \mathbb{Q}$.

We would like to start comparing different extensions of a field K. First, we can use the evaluation homomorphism to classify the simple algebraic extensions up to isomorphism.

Proposition 1.7 *Let E/K and F/K be two field extensions and let $u \in E$ and $v \in F$ be algebraic over K. Then u and v are roots of the same irreducible polynomial $p \in K[x]$ if and only if there is an isomorphism of fields $\psi : K(u) \to K(v)$ such that $\psi(u) = v$ and $\psi(a) = a$ for all $a \in K$.*

PROOF: Assume that u and v are roots of the same irreducible polynomial $f \in K[x]$. Then by Theorem 1.6 ϕ_u and ϕ_v induce isomorphisms $\bar{\phi}_u : K[x]/\langle p \rangle \to K(u)$ and $\bar{\phi}_v : K[x]/\langle p \rangle \to K(v)$ such that $\bar{\phi}_u(x) = u$, $\bar{\phi}_v(x) = v$ and both of these isomorphisms are identities on K. Then $\psi = \bar{\phi}_v \bar{\phi}_u^{-1}$ is the desired homomorphism.

Conversely, assume there exists such an isomorphism $\psi : K(u) \to K(v)$. Then $\psi\phi_u = \phi_v$, so $\ker(\phi_u) = \ker(\phi_v)$. Therefore, u and v are roots of the same monic irreducible polynomial $f \in K[x]$ with $\langle f \rangle = \ker(\phi_u)$. Q.E.D.

Therefore, one consequence of 1.7 is that the extension $K(u)$ is uniquely determined up to isomorphism. Therefore, one usually talks about the field obtained by **adjoining a root** of the irreducible polynomial $p \in K[x]$ to the field K.

Now we have the following theorem that gives us a simple way to conclude that we have an algebraic extension.

Theorem 1.8 *If F is a finite dimensional extension field of K, then F is finitely generated and algebraic over K.*

PROOF: Assume $[F : K] = n$. Then for any $u \in F$ the set $\{1, u, u^2, \ldots, u^n\}$ is a set of $n+1$ elements, hence is linearly dependent. Therefore there exist $a_0, \ldots, a_n \in K$, not all zero, such that

$$a_0 + a_1 u + \cdots + a_n u^n = 0,$$

hence u is algebraic over K. As u was arbitrary, F is algebraic over K. Also, if $\{v_1, \ldots, v_n\}$ is a K-basis of F then it is clear that $F = K(v_1, \ldots, v_n)$, so is finitely generated over K. Q.E.D.

Next, if F/K is an extension of fields and E is a subfield of F containing K, we call E an **intermediate field**.

Theorem 1.9 *Let F/K be a field extension and let E be an intermediate field. Then $[F : K] = [F : E][E : K]$. Furthermore $[F : K]$ is finite if and only if $[F : E]$ and $[E : K]$ are finite.*

PROOF: Let B be a K-basis of E and let B' be a E-basis of F. Then it suffices to show that $BB' = \{xy | x \in B, y \in B'\}$ is a K-basis of F as $|BB'| = |B||B'|$.

First we show BB' spans F. Let $z \in F$. Then there exist $y_1, \ldots, y_n \in B'$ and $a_1, \ldots, a_n \in E$ such that $z = \sum_{i=1}^{n} a_i y_i$. But as each $a_i \in E$, there exist $x_{i,1}, \ldots, x_{i,r_i} \in B$ and $c_{i,1}, \ldots, c_{i,r_i} \in K$ such that $a_i = \sum_{j=1}^{r_i} c_{i,j} x_{i,j}$. Therefore

$$z = \sum_{i=1}^{n} \left(\sum_{j=1}^{r_i} c_{i,j}(x_{i,j} y_i) \right)$$

hence BB' spans F.

Now assume that for some $x_1, \ldots, x_m \in B$, $y_1, \ldots, y_n \in B'$ and $c_{1,1}, c_{1,2}, \ldots, c_{m,n} \in K$ then $\sum_{i=1}^{n} \sum_{j=1}^{m} c_{i,j} x_j y_i = 0$. Then by the independence of B' we get that for every i we have $\sum_{j=1}^{m} c_{i,j} x_j = 0$. But B is independent, so this gives us $c_{i,j} = 0$ for all i, j. Therefore BB' is independent and hence a basis of F over K. Q.E.D.

Note that if $u \in F$ is algebraic over K and E is an intermediate field that it follows from Theorem 1.6 that

$$[E(u) : E] \leq [K(u) : K]$$

Indeed, if $[K(u) : K] = n$, then the minimal polynomial $p \in K[x]$ of u is also a polynomial in $E[x]$. Therefore, u is a root of a polynomial of degree n in $E[x]$ hence the minimal polynomial of u in $E[x]$ must have degree less than or equal to n. We use this observation to prove the following:

Theorem 1.10 *If F/K is an extension of fields and E is an intermediate field such that F is algebraic over E and E is algebraic over K, then F is algebraic over K.*

PROOF: Let $u \in F$. Then, since u is algebraic over E there exists an $n \in \mathbb{N}$ and $b_0, \ldots, b_n \in E$ such that $b_n u^n + \cdots + b_1 u + b_0 = 0$. Now, since E is algebraic over K, each b_j is also algebraic over K and hence is algebraic over every intermediate field between E and K. In particular, we get the following tower of fields:

$$K \subseteq K(b_0) \subseteq K(b_0, b_1) \subseteq \ldots \subseteq K(b_0, \ldots, b_n) \subseteq K(b_0, \ldots, b_n, u)$$

where each extension is a simple algebraic extension of the previous field, hence the degree of each extension is finite by Theorem 1.6. So, by Theorem 1.9, we have

$$[K(b_0, \ldots, b_n, u) : K] = [K(b_0, \ldots, b_n, u) : K(b_0, \ldots, b_n)] \cdots [K(b_0) : K]$$

hence $[K(b_0, \ldots, b_n, u) : K]$ is finite. Now by Theorem 1.8 $K(b_0, \ldots, b_n, u)$ is algebraic over K, hence u must be algebraic over K. Q.E.D.

Theorem 1.11 *Let F/K be a field extension and let E be the set of all elements of F which are algebraic over K. Then E is a subfield of F that is algebraic over K.*

PROOF: Let $u, v \in E$ be nonzero. Then $[K(u,v) : K] = [K(u,v) : K(u)][K(u) : K] \leq [K(v) : K][K(u) : K]$, hence $[K(u,v) : K]$ is finite so by Theorem 1.8 we have $K(u,v)$ is algebraic over K. Therefore $K(u,v) \subseteq E$ and since $u - v, uv \in K(u,v) \subseteq E$, we know E is a subring of F. Furthermore, $u^{-1} \in K(u) \subseteq E$, so every non-zero element of E has an inverse. Therefore, E is a subfield of F that is by definition algebraic over K. Q.E.D.

2 Galois Groups

In this section we introduce Galois groups. Évariste Galois (1812-1832) was interested in using groups to study field extensions defined by polynomials. In particular, he wanted to give a condition that holds precisely when a general formula for the roots of polynomials could be found using only radicals (square roots, cube roots, etc.). His work proved that there was no general formula giving the roots of an arbitrary quintic. (The insolvability of the quintic by radicals was actually proven earlier by Abel, but Galois' techniques have more general applications.) We will try to prove this result in what time remains in the semester.

Let E and F be extension fields of a field K. A nonzero map $\sigma : E \to F$ that is a field homomorphism such that $\sigma(a) = a$ for all $a \in K$ is called a **K-homomorphism**. A K-isomorphism $\sigma : F \to F$ is called a **K-automorphism** of F. We denote the set of all K-automorphisms by Gal(F/K). (Note that we will denote the set of all automorphisms from F to itself by Aut(F). It is fairly easy to show Aut(F) is a group.) Then we have the following lemma and definition.

Lemma 2.1 *The set* Gal(F/K) *is a group under composition. We call this group the* **Galois Group** *of F over K.*

PROOF: We will show that Gal(F/K) is a subgroup of $A(F)$, the group of all bijections from F to F. Clearly $\langle \mathrm{id_F} \rangle \in$ Gal(F/K), so Gal(F/K) is non-empty. Now let $\phi, \theta \in$ Gal(F/K). Then $\phi\theta^{-1}$ is an automorphism of F (as the composition of any two ring isomorphisms is a ring isomorphism) and $\phi\theta^{-1}(a) = \phi(\theta^{-1}(a)) = \phi(a) = a$ for all $a \in K$. Therefore $\phi\theta^{-1} \in$ Gal(F/K) hence by Theorem I.2.5 Gal(F/K) is a group. Q.E.D.

Now we restate a problem from Homework 8 and use it to compute some easy Galois groups.

Theorem 2.2 *Let F/K be a field extension and let $u \in F$ have minimal polynomial $p \in K[x]$. Then $\sigma(u)$ is also a root of p for any $\sigma \in$ Gal(F/K). In other words, any $\sigma \in$ Gal(K/F) must permute the roots of p that are in F.*

PROOF: Problem 3(b) of Homework 8.

Example. Consider $\mathbb{C}$, the field of complex numbers. Then $\mathbb{C} = \mathbb{R}(i)$ and the only roots of x^2+1 are i and $-i$. Therefore, by Theorem 2.2, there are at most two elements in $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. It is easy to verify that complex conjugation is an automorphism of $\mathbb{C}$ that leaves $\mathbb{R}$ fixed, hence $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}_2$ since it contains exactly two elements.

Example. Consider $\mathbb{Q}(\sqrt{5})$ as an extension field of $\mathbb{Q}$. Note that $\sqrt{5}$ and $-\sqrt{5}$ are the two roots of the irreducible polynomial $x^2 - 5 \in \mathbb{Q}[x]$. By Theorem 2.2 there are at most 2 elements of $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$. It is easy to verify that $\sigma : \mathbb{Q}(\sqrt{5}) \to \mathbb{Q}(\sqrt{5})$ given by $\phi(a + b\sqrt{5}) = a - b\sqrt{5}$ is a non-trivial automorphism, hence $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) \cong \mathbb{Z}_2$.

Example. Consider $\mathbb{Q}(\sqrt[3]{5})$. Note that $\sqrt[3]{5}$ is the only real root of $x^3 - 5$ and that $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{5}) \subset \mathbb{R}$. Then by Homework 8 Problem 3(b) there can only be one element of $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{5}/\mathbb{Q})$.

So, to every field extension we can associate a group. Then we would like to know what information the Galois group tells us about the field extension.

We saw that to every field extension F/K we can associate a group Gal(F/K). Now, if there is an intermediate field $K \subset E \subset F$, what can we say about Gal(F/E) in relation to Gal(F/K)?

Theorem 2.3 *Let F/K be a field extension. Then*

1. *For any intermediate field E we have $E' = \mathrm{Gal(F/E)}$ is a subgroup of $\mathrm{Gal(F/K)}$.*
2. *For any subgroup H of $\mathrm{Gal(F/K)}$ we have $H' = \{v \in F | \sigma(v) = v \text{ for all } \sigma \in H\}$ is an intermediate field of F/K.*

Proof: (1) Let E be any intermediate field. Then $\mathrm{Gal(F/E)} = \{\sigma \in \mathrm{Aut(F)} | \sigma(\mathrm{b}) = \mathrm{b} \text{ for all } \mathrm{b} \in \mathrm{E}\} \subseteq \{\sigma \in \mathrm{Aut(F)} | \sigma(\mathrm{a}) = \mathrm{a} \text{ for all } \mathrm{a} \in \mathrm{K}\} = \mathrm{Gal(F/K)}$. Therefore Gal(F/E) is a subgroup of $A(F)$ contained in Gal(F/K), hence $E' = \mathrm{Gal(F/E)} < \mathrm{Gal(F/K)}$.

(2) Let $H < \mathrm{Gal(F/K)}$. As $K \subseteq H'$, H' is non-empty and contains 0 and 1. Then for any $u, v \in H'$ we have $\sigma(u - v) = \sigma(u) - \sigma(v) = u - v$ and $\sigma(uv) = \sigma(u)\sigma(v) = uv$ for all $\sigma \in H$. Therefore $u - v$ and uv are in H' and hence H' is a subring of F. Also, for any $0 \neq u \in H'$ we have $\sigma(u^{-1}) = \sigma(u)^{-1} = u^{-1}$, hence $u^{-1} \in H'$. Therefore H' is a subfield of F containing K. Q.E.D.

If H is a subgroup of Gal(F/K) we will call H' the **fixed field** of H in F. So we have a way of associating to every intermediate field E an subgroup E' of Gal(F/K) and a way of associating to every subgroup H of Gal(F/K) an intermediate field H' between F and K. The natural question arises as to whether this gives us a one-to-one correspondence between the intermediate fields of F/K and the subgroups of Gal(F/K). The answer is no in general, as the example of $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$ shows us. Then we can ask ourselves under what conditions can we get this nice correspondence.

For the field extension F/K we make the following observations about this correspondence (using the prime notation), the proofs of which we leave as exercises.

Observations:

1. $F' = \langle \mathrm{id_F} \rangle$
2. $K' = \mathrm{Gal(F/K)}$
3. $\langle \mathrm{id_F} \rangle' = \mathrm{F}$
4. If L and M are intermediate fields such that $L \subseteq M$ then $M' < L'$.
5. If H and J are subgroups of $\mathrm{Gal(F/K)}$ such that $H < J$, then J' is a subfield of H'.
6. For any intermediate field L and any subgroup $H < \mathrm{Gal(F/K)}$ we have $L \subseteq (L')' = L''$ and $H < (H')' = H''$.
7. For any intermediate field L and any subgroup $H < \mathrm{Gal(F/K)}$ we have $L' = (L'')' = L'''$ and $H' = (H'')' = H'''$.

We can summarize these properties using the following diagram:

$$\begin{array}{ccc} F & \longmapsto & \langle \mathrm{id_F} \rangle \\ \cup & & \wedge \\ M & \longmapsto & M' \\ \cup & & \wedge \\ L & \longmapsto & L' \\ \cup & & \wedge \\ K & \longmapsto & \mathrm{Gal(F/K)} \end{array} \qquad\qquad \begin{array}{ccc} \mathrm{Gal(F/K)} & & K \\ \vee & & \cap \\ J & \longmapsto & J' \\ \vee & & \cap \\ H & \longmapsto & H' \\ \vee & & \cap \\ \langle \mathrm{id_F} \rangle & \longmapsto & F \end{array}$$

Note that Observation (6) gives us that $L \subseteq L''$ for any intermediate field L and $H < H''$ for any subgroup $H < \mathrm{Gal(F/K)}$. We will define an intermediate field L to be **closed** if $L = L''$. Similarly, we will define the subgroup $H < \mathrm{Gal(F/K)}$ to be **closed** if $H = H''$.

Theorem 2.4 *Let F/K be a field extension. Then there is a one-to-one correspondence between the closed intermediate fields and the closed subgroups of* $\mathrm{Gal(F/K)}$ *given by $E \mapsto E' <$* $\mathrm{Gal(F/K)}$ *for any intermediate field E.*

Proof: First we show this correspondence is injective. Let E and L be two intermediate fields such that $E' = L'$. Then since E and L are closed, $E = E'' = L'' = L$. To show this correspondence is surjective, note that for any closed subgroup $H < \mathrm{Gal(F/K)}$ we have $H = H'' = (H')'$, hence corresponds to the intermediate field H'. Q.E.D.

One important thing to note here is that $\mathrm{Gal(K/F)'}$ is not necessarily K and could potentially be larger than K. In other words, K itself might not be closed. This motivates the following definition.

Definition 2.5 *Let F/K be a field extension. Then F is said to be* **Galois** *over K if* $\mathrm{Gal(F/K)' = K}$. *In this case we call F/K a* **Galois extension** *of K.*

3 Galois Groups of Polynomials

As Galois was interested in finding roots of polynomials, we take some time to examine fields that are defined in terms of roots of polynomials.

Note that all of the examples in the previous section were gotten by adjoining roots of some irreducible polynomial to our subfield (i. e. , all of these extensions are simple algebraic extensions). Let us take some time to study algebraic extensions that are built up from these simple extensions.

Definition 3.1 *Let K be a field and let $f \in K[x]$ have degree n. An extension field F/K is called a* **splitting field** *for f over K if there exist elements $r_1, \ldots, r_n \in F$ such that $f(x) = a(x - r_1) \cdots (x - r_n)$ for some $a \in K$ and $F = K(r_1, \ldots, r_n)$.*

Theorem 3.2 *Let $f \in K[x]$ have degree $n > 0$. Then there exists a splitting field F of f over K and $[F : K] \leq n!$.*

Proof: Let us induct on n. If $n = 1$, K is a splitting field for f over K, hence we are done. Now assume our theorem is true for any field L containing K and for any $g \in L[x]$ such that $\deg(g) < n$. Now let p be an irreducible factor of f in $K[x]$ and let r_1 be a root of p. Then f has a root in $K(r_1)$, hence as an element of $K(r_1)[x]$, $f = (x - r_1)g$ for some $g \in K(r_1)[x]$ of degree $n-1$. Therefore by our induction hypothesis, there exists a splitting field $F/K(r_1)$ of g over $K(r_1)$ such that $[F : K(r_1)] \leq (n-1)!$. Then you can check that F is a splitting field of f using Problem 2(a) of Homework 8. Also, $[F : K] = [F : K(r_1)][K(r_1) : K] \leq (n-1)!n = n!$ by Theorems 1.9 and 1.6. Q.E.D.

Note that since by Problem 2 of Homework 8 we have $K(r_1, \ldots, r_n) = K(r_1)(r_2) \cdots (r_n)$, the uniqueness (up to isomorphism) of the splitting fields of f follows from Proposition 1.7. (The argument is a little tricky, so we note that one usually uses Theorem 5.6 to prove the uniqueness of a splitting field.)

Definition 3.3 *Let $f \in K[x]$ have degree $n > 0$. The* **Galois group of f over K** *is* $\mathrm{Gal(F/K)}$ *where F is a splitting field of f.*

Example. From our above examples, it is clear that $\mathbb{C}$ is a splitting field of $x^2 + 1$ over $\mathbb{R}$, hence the Galois group of $x^2 + 1$ over $\mathbb{R}$ is isomorphic to $\mathbb{Z}_2$. Similarly, the Galois group of $x^2 - 5$ over $\mathbb{Q}$ is also isomorphic to $\mathbb{Z}_2$.

Example. Let us look at the splitting field and Galois group of $f = x^3 + 4$ over $\mathbb{Z}_5$. Then $f = x^3 - 1 = (x - 1)(x^2 + x + 1)$ in $\mathbb{Z}_5[x]$. Therefore a splitting field of f over $\mathbb{Z}_5$ is also a

splitting field for the irreducible polynomial $p = x^2+x+1$ over $\mathbb{Z}_5$. Let u be a root of p in some extension field of $\mathbb{Z}_5$. Then $\mathbb{Z}_5(u)$ is a splitting field for p since $p = (x-u)(x-u') \in \mathbb{Z}_5(u)[x]$ for some $u' \in \mathbb{Z}_5(u)$. (This follows since p is in the kernel of the evaluation homomorphism $\phi_u : \mathbb{Z}_5(u)[x] \to \mathbb{Z}_5(u)$, hence is divisible by $x-u$, the generator of $\ker(\phi_u)$.) Furthermore, since 2 is invertible in $\mathbb{Z}_5$ and $[\mathbb{Z}_5(u) : \mathbb{Z}_5] = 2$, by Homework 8 Problem 3(c) there are exactly two elements in $\mathrm{Gal}(\mathbb{Z}_5(\mathrm{u})/\mathbb{Z}_5)$, hence $\mathrm{Gal}(\mathbb{Z}_5(\mathrm{u})/\mathbb{Z}_5) \cong \mathbb{Z}_2$.

Before going on to more sophisticated examples, need one more lemma.

Lemma 3.4 *Let F/K be a finite-dimensional extension and let $L \subseteq E$ be intermediate fields. Then $[L' : E'] \leq [E : L]$. In particular, $|\mathrm{Gal(F/K)}| \leq [\mathrm{F} : \mathrm{K}]$.*

PROOF: We induct on $n = [E : L]$. Note if $n = 1$ we are done. So assume $n > 1$ and the theorem is true for all $j < n$. Choose $u \in E$ such that $u \notin L$. As $[E : L]$ is finite, u is algebraic over L by Theorem 1.8 with minimal polynomial $p \in L[x]$ of degree $k > 1$. By Theorems 1.6 and 1.9 we have $[L(u) : L] = k$ and $[E : L(u)] = n/k$. If $k < n$ then $1 < (n/k) < n$ so by induction $[L' : E'] = [L' : L(u)'][L(u)' : E'] \leq k(n/k) = n = [E : L]$, hence we are done.

Now assume $k = n$ so that $E = L(u)$. Let us construct an injective map from the set S of left cosets of E' in L' to the set T of distinct roots of the minimal polynomial $p \in L[x]$ of u. (We note that since $\deg(\mathrm{p}) = \mathrm{n}$, the set T contains at most n elements.)

Let $\tau E'$ be a left coset of E' in L'. Then define a map $\psi : S \to T$ by letting $\psi(\tau E') = \tau(u)$. Note that ψ is well defined since if $\tau E' = \sigma E'$ then $\sigma = \tau\rho$ for some $\rho \in E'$. Therefore $\sigma(u) = \tau\rho(u) = \tau(u)$ since $u \in E$ implies $\rho(u) = u$. To show ψ is one-to-one, assume $\tau(u) = \sigma(u)$. By Theorem 1.6 for any $w \in E$ we have $w = \sum_{i=0}^{n-1} a_i u^i$ for some $a_0, \ldots, a_{n-1} \in L$. Therefore $\sigma^{-1}\tau(w) = \sum_{i=0}^{n-1} a_i \sigma^{-1}\tau(u)^i = \sum_{i=0}^{n-1} a_i u^i = w$, hence $\sigma^{-1}\tau \in E'$. Therefore, ψ is one-to-one, hence $[L' : E'] = |S| \leq |T| \leq n = [E : L]$.

Finally, taking $L = K$ and $E = F$ we get $|\mathrm{Gal(F/K)}| \leq [\mathrm{F} : \mathrm{K}]$. Q.E.D.

So we consider the following example. We note that a similar example is done in a little more detail in Example 8.3.2 of Beachy and Blair (2nd Edition).

Example. Let us look at the splitting field and Galois group of $f = x^3 - 5$ over $\mathbb{Q}$. Clearly $\mathbb{Q}(\sqrt[3]{5})$ contains a root of f but is not a splitting field for f since $\mathbb{Q}(\sqrt[3]{5})$ only contains one root of f. Then, in $\mathbb{Q}(\sqrt[3]{5})[x]$ we have $f = (x - \sqrt[3]{5})(x^2 + \sqrt[3]{5}x + \sqrt[3]{25})$ and the quadratic factor is irreducible over $\mathbb{Q}(\sqrt[3]{5})$. So let $\zeta = (-1+i\sqrt{3})\sqrt[3]{5}/2$. Then ζ is a root of f over $\mathbb{Q}$, hence is a root of $(x^2+\sqrt[3]{5}x+\sqrt[3]{25})$ over $\mathbb{Q}(\sqrt[3]{5})$. Then it becomes clear that $F = \mathbb{Q}(\sqrt[3]{5}, \zeta)$ is a splitting field of $x^3 - 5$ over $\mathbb{Q}$. Furthermore, $[F : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{5}, \zeta) : \mathbb{Q}(\sqrt[3]{5})][\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 2 \cdot 3 = 3!$ by Theorems 1.9 and 1.6.

To compute the Galois group, by Theorem 2.2 any element of the Galois group must permute the roots $\sqrt[3]{5}, \zeta, \bar{\zeta}$ where $\bar{\zeta}$ denotes the complex conjugate of ζ. So let $\sigma, \tau \in \mathrm{Gal(F/\mathbb{Q})}$ be defined by letting τ correspond to complex conjugation and let σ correspond

to a cyclic permutation of the roots. So $\sigma(\sqrt[3]{5}) = \zeta, \sigma(\zeta) = \bar{\zeta}, \sigma(\bar{\zeta}) = \sqrt[3]{5}$ and $\sigma(q) = q$ for all $q \in \mathbb{Q}$. We leave it as an exercise to show that σ is an automorphism. Clearly σ has order 3 and τ has order 2. Furthermore, $\sigma\tau(\zeta) = \sqrt[3]{5}$ while $\tau\sigma(\zeta) = \zeta$, so Gal(F/K) is noncommutative. Finally, by Lemma 3.4 it follows that $|\mathrm{Gal}(\mathrm{F}/\mathbb{Q})| = 6$, hence $\mathrm{Gal}(\mathrm{F}/\mathbb{Q}) \cong \mathrm{S}_3$.

Before computing other Galois groups, it will be useful to prove the Fundamental Theorem of Galois Theory.

4 The Fundamental Theorem

Our goal for this section is to prove the Fundamental Theorem of Galois Theory, the first part of which we now state.

Theorem 4.1 (Fundamental Theorem of Galois Theory, Part I) *Let F/K be a finite-degree Galois extension. Then there exists a one-to-one correspondence between the set of all intermediate fields and the set of subgroups of* Gal(F/K) *given by $E \mapsto E' <$ Gal(F/K) for all intermediate fields E. Furthermore, for any two intermediate fields $E \subseteq L$ we have $[L : E] = [E' : L']$.*

Before proving this part of the Fundamental Theorem, we note that to get a one-to-one correspondence between intermediate fields and subgroups, by Theorem 2.4 it suffices to prove that for any intermediate field E we have $[E'' : E] = 1$ and for any subgroup $H <$ Gal(F/K) we have $[H'' : H] = 1$. We will concentrate on proving various inequalities involving indices and degrees. We start with the following lemma.

Lemma 4.2 (Artin) *Let F/K be an extension of finite degree. Then for any subgroups $H < J <$ Gal(F/K) we have $[H' : J'] \leq [J : H]$.*

Proof: Let $n = [J : H]$ and choose $n+1$ elements $u_1, \ldots, u_{n+1} \in H'$. Now we need to show that these elements are linearly dependent over J'. Note that in our proof we may assume no u_i is zero (otherwise $\{u_1, \ldots, u_{n+1}\}$ would be linearly dependent and we are done).

Let $\{\tau_1 = \mathrm{id}_\mathrm{F}, \tau_2, \ldots, \tau_\mathrm{n}\} \subseteq$ J be a complete set of left coset representatives of H in J. Then we consider the homogeneous system of n linear equations in $n+1$ unknowns given by

$$\begin{array}{rcl} \tau_1(u_1)x_1 + \cdots + \tau_1(u_{n+1})x_{n+1} & = & 0 \\ \tau_2(u_1)x_1 + \cdots + \tau_2(u_{n+1})x_{n+1} & = & 0 \\ \vdots & & \vdots \\ \tau_n(u_1)x_1 + \cdots + \tau_n(u_{n+1})x_{n+1} & = & 0 \end{array} \tag{1}$$

Such a system always has a non-trivial solution in H' (i. e. , a solution different from $x_1 = x_2 = \cdots = x_{n+1} = 0$). Note that we will be finished if we can prove that there exists a non-trivial solution to this system in J'. Indeed, any such solution $x_1 = c_1, \ldots, x_{n+1} = c_{n+1}$

in J' would imply linear dependence over J' since it would have to be a solution to the first equation of our system (recall we defined $\tau_1 = \mathrm{id_F}$).

So choose a non-trivial solution $x_1 = c_1, \ldots, x_{n+1} = c_{n+1}$ to the system (1) that has the least number of the c_j being non-zero. We can re-order our u_i so that $c_1, \ldots, c_r$ are non-zero and $c_{r+1} = \cdots = c_{n+1} = 0$. We can also assume that $c_1 = 1$.

As J acts on the left cosets of H by left translation, for any $\sigma \in J$ the set $\{\sigma\tau_1, \ldots, \sigma\tau_n\}$ is another complete set of left coset representatives of H in J. Therefore, for each $1 \leq i \leq n$ there exists a $1 \leq k_i \leq n$ such that $\sigma\tau_i \in \tau_{k_i}H$. Therefore for any $1 \leq j \leq n+1$ since $u_j \in H'$ we have $\sigma\tau_i(u_j) = \tau_{k_i}h(u_j) = \tau_{k_i}(u_j)$ for some $h \in H$.

Then for any $1 \leq i \leq n$ we get from the system (1) that $0 = \sigma\left(\sum_{j=1}^{n+1} \tau_i(u_j)c_j\right) = \sum_{j=1}^{n+1} \sigma\tau_i(u_j)\sigma(c_j)$. Therefore $x_1 = \sigma(c_1) = \sigma(1) = 1, x_2 = \sigma(c_2), \ldots, x_{n+1} = \sigma(c_{n+1})$ must be a solution to the system of equations

$$\begin{array}{rcl} \tau_{k_1}(u_1)x_1 + \cdots + \tau_{k_1}(u_{n+1})x_{n+1} & = & 0 \\ \tau_{k_2}(u_1)x_1 + \cdots + \tau_{k_2}(u_{n+1})x_{n+1} & = & 0 \\ \vdots & & \vdots \\ \tau_{k_n}(u_1)x_1 + \cdots + \tau_{k_n}(u_{n+1})x_{n+1} & = & 0 \end{array} \tag{2}$$

But since $\{\tau_{k_1}, \ldots, \tau_{k_n}\}$ is a complete set of left coset representatives of H, it must be equal to $\{\tau_1, \ldots, \tau_n\}$, hence the homogeneous system (2) is really the same system as (1). Therefore $x_1 = \sigma(c_1) = 1, x_2 = \sigma(c_2), \ldots, x_{n+1} = \sigma(c_{n+1})$ is also a solution to system (1).

Finally, by the properties of solutions of homogeneous systems, $x_1 = c_1 - \sigma(c_1) = 0, x_2 = c_2 - \sigma(c_2), \ldots, x_{n+1} = c_{n+1} - \sigma(c_{n+1})$ is also a solution to (1) with less non-zero terms than $x_1 = c_1, \ldots, x_{n+1} = c_{n+1}$. Hence by minimality of the number of non-zero terms, we get $\sigma(c_i) = c_i$ for all $1 \leq i \leq n+1$. In other words, $c_1, \ldots, c_{n+1} \in J'$ so $\{u_1, \ldots, u_{n+1}\}$ must be linearly dependent over J'. Q.E.D.

Proof of Part I of Fundamental Theorem: To get our one-to-one correspondence between intermediate fields and subgroups of Gal(F/K) by Theorem 2.4 we only need to show that all intermediate fields and subgroups are closed.

So let E be any intermediate field. Then by Observation (6) we have $E \subseteq E''$. Now since F/K is a Galois extension, $K'' = K$ so we get by Lemmas 3.4 and 4.2 that $[E'' : K] \geq [E : K] \geq [K' : E'] \geq [E'' : K''] = [E'' : K]$. Therefore, by Theorem 1.9 we have $[E'' : E] = [E'' : K]/[E : K] = 1$ so E is closed.

Now choose $H < \mathrm{Gal(F/K)}$. Then it follows from Observations (1), (3), and (6) that $\langle \mathrm{id_F} \rangle$ is closed and $H < H''$. Therefore, by Lemmas 3.4 and 4.2 we have $[H'' : \langle \mathrm{id_F} \rangle] \geq [\mathrm{H} : \langle \mathrm{id_F} \rangle] \geq [\langle \mathrm{id_F} \rangle', \mathrm{H}'] \geq [\mathrm{H}'' : \langle \mathrm{id_F} \rangle''] = [\mathrm{H}'' : \langle \mathrm{id_F} \rangle]$. Therefore, by Lagrange's Theorem, $[H'' : H] = [H'' : \langle \mathrm{id_F} \rangle]/[\mathrm{H} : \langle \mathrm{id_F} \rangle] = 1$ so H is closed.

Finally, for any two intermediate fields $L \subseteq E$, we have that $[E : L] \geq [L' : E'] \geq [E'' : L''] = [E : L]$. Q.E.D.

Therefore by examining the Galois group of a Galois extension, we can determine all of the intermediate fields of the extension by looking at the subgroups of the Galois group. Furthermore, as we saw in the previous section, this result can help us compute Galois groups of polynomials.

Another observation to make is that for any Galois extension F/K and any intermediate field E, it follows that $E' = \mathrm{Gal(F/E)}$. The question remains whether we can use E' to determine Gal(E/K). One problem that can occur here is that E might not be Galois over K. For example, consider the tower of fields $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{5}) \subseteq F$ where F is a splitting field for $x^3 - 5$ over $\mathbb{Q}$. The second part of the Fundamental Theorem addresses this issue.

So let E be an intermediate field of an extension F/K. We say that E is **stable** relative to F/K if for every $\sigma \in \mathrm{Gal(F/K)}$, $\sigma(E) \subseteq E$. This implies that by restricting σ to E we get an automorphism of E whose inverse is the restriction of σ^{-1} to E.

Lemma 4.3 *Let F/K be an extension and let E be a stable intermediate field. Then there exists a homomorphism $\Psi : \mathrm{Gal(F/K)} \to \mathrm{Gal(E/K)}$ with kernel $E' = \mathrm{Gal(F/E)}$.*

Proof: For any $\sigma \in \mathrm{Gal(F/K)}$ define $\Psi(\sigma) = \sigma|_E$. As E is stable, $\Psi(\sigma) \in \mathrm{Gal(E/K)}$. It is also clear that Ψ is a homomorphism. Finally $\sigma \in \ker(\Psi) \Leftrightarrow \sigma|_E = \mathrm{id_E} \Leftrightarrow \sigma \in \mathrm{E'}$. Q.E.D.

Lemma 4.4 *Let F/K be an extension.*

1. *If E is a stable intermediate field, then $E' \lhd \mathrm{Gal(F/K)}$.*
2. *If $H \lhd \mathrm{Gal(F/K)}$, then H' is a stable intermediate field.*

Proof: (1) This follows from Lemma 4.3 since E' is the kernel of Ψ.

(2) Let $\sigma \in \mathrm{Gal(F/K)}$ and $u \in H'$. Then for any $\tau \in H$ we have $\sigma^{-1}\tau\sigma \in H$, hence $\sigma^{-1}\tau\sigma(u) = u$. Therefore $\tau(\sigma(u)) = \sigma(u)$ so $\sigma(u) \in H'$ and H' is a stable intermediate field. Q.E.D.

Theorem 4.5 (Fundamental Theorem of Galois Theory, Part II) *Let F/K be a finite-dimensional Galois extension. Then F is Galois over every intermediate field E. Furthermore E is Galois over K if and only if $E' \lhd \mathrm{Gal(F/K)}$, in which case $\mathrm{Gal(E/K)} \cong \mathrm{Gal(F/K)/E'}$.*

Proof: Note that F being Galois over E follows from Part I of the Fundamental Theorem since E is closed. Furthermore, if $E' \lhd \mathrm{Gal(F/K)}$ then $E = E''$ is a stable intermediate field. Therefore, we need to show that the fixed field of Gal(E/K) is K. But for any $u \in E$ with $u \notin K$ there exists $\sigma \in \mathrm{Gal(F/K)}$ such that $\sigma(u) \neq u$, hence $\Psi(\sigma)(u) \neq u$ where $\Psi : \mathrm{Gal(F/K)} \to \mathrm{Gal(E/K)}$ is the homomorphism given in Lemma 4.3. Therefore the fixed field of Gal(E/K) is K so E is Galois over K.

Conversely, if E is Galois over K by Lemma 4.4 it is sufficient to show that E is stable. So let $u \in E$. Then u is algebraic over K since $[E : K]$ is finite (Theorem 1.8), so u has a minimal polynomial $p \in K[x]$. Let $u = u_1, \ldots, u_r$ be the distinct roots of p in E. Clearly $r \leq n = \deg(\mathrm{p})$ and Theorem 2.2 gives us that any $\tau \in \mathrm{Gal(E/K)}$ must simply permute the u_i. This implies that the coefficients of the monic polynomial $g(x) = (x-u_1)(x-u_2)\cdots(x-u_r) \in E[x]$ are fixed by every $\tau \in \mathrm{Gal(E/K)}$, hence $g \in K[x]$. As $g(u) = 0$, $g \in \ker(\phi_u) = \langle p \rangle$ and $\deg(\mathrm{g}) \leq \deg(\mathrm{p})$. As g is monic, we get $g = p$. Consequently, all the roots of p are distinct and lie in E. Therefore, for any $\sigma \in \mathrm{Gal(F/K)}$ we have $\sigma(u)$ is a root of p, hence $\sigma(u) \in E$. This gives us that E is stable, hence $E' \lhd \mathrm{Gal(F/K)}$.

Finally if E is Galois over K we need to show $\mathrm{Gal(E/K)} \cong \mathrm{Gal(F/K)/E'}$. By the First Isomorphism Theorem and Lemma 4.3, it suffices to show Ψ is surjective. But $|\mathrm{Gal(F/K)/E'}| = [\mathrm{Gal(F/K)} : \mathrm{E'}] = [\mathrm{E} : \mathrm{K}] = |\mathrm{Gal(E/K)}|$ by Part I of the Fundamental Theorem. Therefore $\mathrm{Im}(\Psi) = \mathrm{Gal(E/K)}$, hence $\mathrm{Gal(E/K)} \cong \mathrm{Gal(F/K)/E'}$. Q.E.D.

Note that the following corollary follows from the second paragraph of the above proof. This corollary motivates the definition that follows.

Corollary 4.6 *Let F/K be a finite Galois extension and let $p \in K[x]$ be irreducible. If there exists a root of p in F then the roots of p are distinct and all the roots are contained in F.*

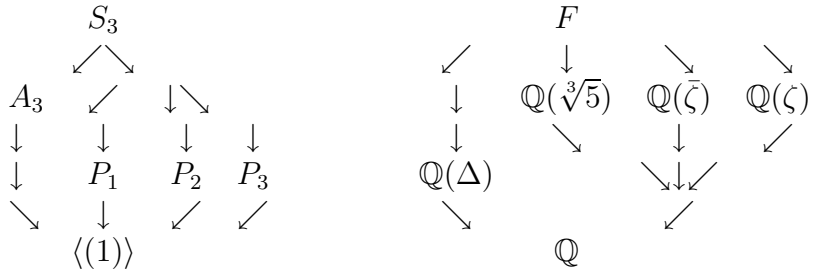
Definition 4.7 *Let K be a field. A polynomial $f \in K[x]$ is* **separable** *if all its irreducible factors have distinct roots in a splitting field for f. The field K is* **perfect** *if every (irreducible) polynomial in $K[x]$ is separable. An algebraic extension F/K is* **separable** *if the minimal polynomial of every element of F is separable. An algebraic extension F/K is* **normal** *if for every $u \in F$, F contains a splitting field for the minimal polynomial of u.*

So Corollary 4.6 can be rephrased to say that every finite Galois extension is a finite separable normal extension. In the next section we prove that the converse is true as well.

We close this section with another look at the example of the splitting field of $x^3 - 5$ over $\mathbb{Q}$.

Example. Now that we have the Fundamental Theorem of Galois Theory, we can describe all the intermediate fields of the extension $F/\mathbb{Q}$ where F is the splitting field of $x^3 - 5$ over $\mathbb{Q}$. We will use the same notation as before. First we list the subgroups of $S_3 = \langle \sigma, \tau \rangle$. Check that $\tau\sigma = \sigma^{-1}\tau$. Then we have $A_3 = \langle \sigma \rangle \lhd S_3$ and 3 Sylow 2-subgroups $P_1 = \langle \tau \rangle$, $P_2 = \langle \sigma\tau \rangle$, and $P_3 = \langle \sigma^2\tau \rangle$. Then by the Fundamental Theorem, there exist exactly four (proper) intermediate fields which must be the fixed fields of each subgroup. Only A_3' is Galois over $\mathbb{Q}$ and must be an extension of degree $[S_3 : A_3] = 2$. Hence we get a picture that

roughly looks like



where $\Delta = (\sqrt[3]{5} - \zeta)(\sqrt[3]{5} - \bar{\zeta})(\zeta - \bar{\zeta})$. Note that of all the intermediate fields only $\mathbb{Q}(\Delta)$ is Galois over $\mathbb{Q}$ and $\mathrm{Gal}(\mathbb{Q}(\Delta)/\mathbb{Q}) = \langle \tau|_{\mathbb{Q}(\Delta)} \rangle \cong \mathbb{Z}_2$.

5 Separable and Normal Extensions

We would like to get a better understanding of when a finite dimensional field extension F/K is Galois. We noted in Corollary 4.6 that all finite-dimensional Galois extensions are normal and separable extensions. Our goal is to prove the converse of Corollary 4.6.

It turns out that in most of the examples we look at, all irreducible polynomials are separable. First we make the following definitions.

Definition 5.1 *Let K be a field. The* **prime subfield** *of K is the smallest subfield of K. If the prime subfield of K has order p for some prime p we say that K has* **characteristic** *p. If the prime subfield of K is infinite, we say K has* **characteristic zero**.

We note that prime subfields must either be isomorphic to $\mathbb{Z}_p$ for some prime p if K has positive characteristic, or isomorphic to $\mathbb{Q}$ if the characteristic of K is zero. If K has characteristic p for some prime p, then $0 = pa = a + \cdots + a$ (p times) for all $a \in K$. One quirk of a field K of characteristic $p > 0$ is that for any $a, b \in K$ we have $(a+b)^p = a^p + b^p$, since p divides all the other binomial coefficients. Therefore, in such a K we have $x^p + 1 = (x+1)^p$ is never irreducible.

Definition 5.2 *Let $f \in K[x]$ with $f = \sum_{j=0}^{n} a_j x^j$. The* **formal derivative** *$f'(x)$ of $f(x)$ is the polynomial*

$$f'(x) = \sum_{j=1}^{n} j a_j x^{j-1}$$

where $ja_j = a_j + \cdots + a_j$ (j times).

Note that for polynomials in $\mathbb{R}[x]$, this definition agrees with the usual derivative taught in a first year calculus course. Therefore, we can use this analogy to prove that the product and chain rules also hold for formal derivatives.

Proposition 5.3 *A polynomial $f(x) \in K[x]$ has a multiple root if and only if $f(x)$ and $f'(x)$ have a common root.*

PROOF: Let F be a splitting field for $f(x)$ over K. If $f(x)$ has a multiple root $r \in F$, then $f(x) = (x-r)^2 g(x)$ for some $g(x) \in F[x]$. Therefore $f'(x) = 2(x-r)g(x) + (x-r)^2 g'(x)$ hence $f'(r) = 0$.

Now assume $f(x)$ has no multiple roots. Then $f(x) = a(x-r_1)(x-r_2)\cdots(x-r_n)$ for some $a \in K$ and *distinct* $r_1, \ldots, r_n \in F$. Then

$$f'(x) = a(x-r_2)\cdots(x-r_n) + a(x-r_1)(x-r_3)\cdots(x-r_n) + \cdots + a(x-r_1)(x-r_2)\cdots(x-r_{n-1})$$

Therefore for any j we have $f'(r_j) = a(r_j - r_1)\cdots(r_j - r_{j-1})(r_j - r_{j+1})\cdots(r_j - r_n) \neq 0$ since each factor is nonzero. Therefore $f(x)$ and $f'(x)$ have no common roots in F. Q.E.D.

Proposition 5.4 *Let $f(x) \in K[x]$ be irreducible. If f is not separable then the characteristic K is $p > 0$ for some prime p and f has the form $f(x) = \sum_{i=0}^{n} a_{ip} x^{ip}$.*

PROOF: Let f be irreducible over $K[x]$ and let F be a splitting field of f over K. If $r \in F$ is a multiple root of $f(x)$, then $\langle f \rangle$ is the kernel of the evaluation homomorphism $\phi_r : K[x] \to F$. By Proposition 5.3, $f'(r) = 0$ so $f'(x) \in \langle f \rangle$. As deg(f′) < deg(f), we get $f'(x) = 0$. This is impossible over a field of characteristic zero (as deg(f) ≥ 1), hence char(K) = p > 0 for some prime p. Now the result follows. Q.E.D.

Corollary 5.5 *If K is a field of characteristic zero, then every irreducible polynomial over K is separable.*

Therefore, any splitting field of a polynomial over a field of characteristic zero is a Galois extension. We comment here that this corollary is true for any finite field as well. We refer the reader to Beachy/Blair Theorem 8.2.6 and Corollary 8.2.7 for the proof of this.

Let p be a prime and let u be transcendental over $\mathbb{Z}_p$. Then the polynomial $x^p - u$ is **not** separable over $\mathbb{Z}_p(u)$ since if r is a root of $x^p - u$, we get $x^p - u = (x-r)^p$ since $\mathbb{Z}_p(u)$ has characteristic p.

Now let us devote some effort to proving the converse of Corollary 4.6. We start with the following useful theorem. This theorem is based on the result that any isomorphism of fields $\sigma : K \to L$ defines a ring isomorphism $\sigma_x : K[x] \to L[x]$ where $\sigma_x(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \sigma(a_i) x^i$. We leave it as an exercise to check this is a ring isomorphism.

Theorem 5.6 *Let $\sigma : K \to L$ be an isomorphism of fields and let $f = \sum_{i=0}^{n} a_i x^i \in K[x]$ be a separable polynomial of degree $n > 0$. If F is a splitting field of f over K and E is a splitting field of $\sigma_x f = \sum_{i=0}^{n} \sigma(a_i) x^i$ over L, then there exist exactly $[F : K]$ isomorphisms $\tilde{\sigma} : F \to E$ that extend σ.*

NOTE: We say $\tilde{\sigma}$ **extends** σ if $\tilde{\sigma}(a) = \sigma(a)$ for all $a \in K$.

PROOF: We induct on $m = [F : K]$. If $m = 1$, $F = K$ so f splits over K, hence σf splits over L, so $L = E$. So take $\tilde{\sigma} = \sigma$. Now assume the theorem is true for all fields K and all polynomials $h(x) \in K[x]$ such that the splitting field of h has degree less than m over K. As $[F : K] = m > 1$, the polynomial f must have an irreducible factor g of degree $d > 1$. Let $u \in F$ be a root of g. Then $\sigma_x g$ must be irreducible over L as $\sigma_x : K[x] \to L[x]$ is a ring isomorphism. Note that we can define a composition of ring homomorphisms

$$K[x] \xrightarrow{\sigma_x} L[x] \xrightarrow{\pi} L[x]/\langle \sigma_x g \rangle$$

whose kernel is $\langle g \rangle$. Therefore by Theorem 1.6 and the First Isomorphism Theorem for rings we get

$$K(u) \cong K[x]/\langle g \rangle \cong L[x]/\langle \sigma_x g \rangle \cong L(v)$$

where $v \in E$ is any root of $\sigma_x g$. Therefore, if $\{v_1, \ldots, v_d\}$ is the set of roots of $\sigma_x g$, it follows from Proposition 1.7 that there are exactly d field isomorphisms $\tau_j : K(u) \to L(v_j)$ that extend σ where τ_j is uniquely determined by letting $\tau_j(u) = v_j$. As $[K(u) : K] = d > 1$ by Theorem 1.6, we have by Theorem 1.9 that $[F : K(u)] = (m/d) < m$, F is a splitting field for f over $K(u)$ and for each $1 \leq j \leq d$, E is a splitting field for $\sigma_x f$ over $L(v_j)$. So we apply our induction hypothesis to get that for each $1 \leq j \leq d$, there exist $m/d = [F : K(u)]$ isomorphisms $\omega : F \to E$ that extend τ_j. Therefore, we have $d(m/d) = [F : K]$ isomorphisms that extend σ. Q.E.D.

Hence we get the following theorem.

Theorem 5.7 *Let F/K be an extension. Then the following are equivalent:*

1. *F/K is a finite Galois extension.*
2. *F/K is a finite, normal, separable extension.*
3. *F is the splitting field over K of some separable polynomial.*

PROOF: (1) $\Rightarrow$ (2): Corollary 4.6.

(2) $\Rightarrow$ (3): As F/K is finite, we can choose a K-basis, say $\{v_1, \ldots, v_n\} \subseteq F$ of F. For each $1 \leq i \leq n$, let $f_i \in K[x]$ be the minimal polynomial of v_i over K. Then f is separable over K since F/K is separable, hence each of the f_i are separable over K. Also F is a splitting field for $f = f_1 f_2 \cdots f_n$ since F/K is normal and hence contains all the roots of the f_i, hence all the roots of f.

(3) $\Rightarrow$ (1): Let F be the splitting field over K of some separable polynomial $f \in K[x]$. Let $G = \mathrm{Gal(F/K)}$. Then $G = \mathrm{Gal(F/K'')}$ and F is a splitting field for f over K'' as well. Therefore, by Theorem 5.6, we get $[F : K] = |\mathrm{Gal(F/K)}| = |\mathrm{Gal(F/K'')}| = [\mathrm{F : K''}]$. Hence

$K = K''$ and so F/K is a finite Galois extension. Q.E.D.

Therefore all we need to do to create a finite Galois extension is to look at splitting fields for separable polynomials.

We end this section with the Primitive Element Theorem, which tells us that all finite separable extensions are simple. Note that I do not plan to cover this result in class, but I include it as a supplement to the lectures. First we need a preliminary lemma.

In class, we proved that the group of units $\mathbb{Z}_p^\times$ is cyclic for any prime p. We have the same result for any finite field F. We repeat the proof here.

Lemma 5.8 *Let F be a finite field. Then the group of units $F^\times = F \setminus \{0\}$ is a cyclic group.*

PROOF: Let m be the maximal (multiplicative) order of an element of $F^\times$. By the Fundamental Theorem of Finitely Generated Abelian Groups, the order of any element of $F^\times$ must divide m. In particular, $x^m = 1$ has $|F^\times|$ solutions, hence $|F^\times| \leq \deg(x^m - 1) = m$. But m is the order of an element in $|F^\times|$, hence $m = |F^\times|$ so $F^\times$ must be cyclic. Q.E.D.

We use this lemma to prove the Primitive Element Theorem.

Theorem 5.9 (Primitive Element Theorem) *Let F/K be a finite separable extension. Then $F = K(u)$ for some $u \in F$.*

PROOF: If K is a finite field, then F must also be finite. By Lemma 5.8, $F^\times$ is cyclic. Therefore, if u is a generator for $F^\times$, we get $K = F(u)$.

Now assume K is infinite and $[F : K] = n$ (so F is algebraic over K). Then for any K-basis $v_1, \ldots, v_n \in F$, we have $F = K(v_1, \ldots, v_n)$. Furthermore, $F = K(v_1, \ldots, v_{n-1})(v_n)$ by Homework 8, Problem 2. Therefore, by induction, we can assume $F = K(u, v)$.

Let $p, q \in K[x]$ be the minimal polynomials over K of u and v, respectively. Let $n =$ deg(p) and $m =$ deg(q). Choose an extension E/F such that p and q split in E. As F is separable over K, the roots $u = u_1, u_2, \ldots, u_n$ of p and the roots $v = v_1, v_2, \ldots, v_m$ of q are distinct. Therefore, $w_{i,j} = (u - u_i)/(v - v_j) \in E$ for all $1 \leq i \leq n$ and all $2 \leq j \leq m$.

As K is infinite, we can choose an $a \in K$ such that $a \neq -w_{i,j}$ for any i, j. We want to show $F = K(w)$ for $w = u + av$. Clearly $K(w) \subseteq K(u, v) = F$. Let g be the minimal polynomial of v over $K(w)$. Then the polynomial $h(x) = p(w - ax) \in K(w)$ has v as a root, hence $g|h$. As v was defined to be a root of $q(x)$, $g|q$ as well. Therefore, g must be a product $(x - v)(x - v_1') \cdots (x - v_k')$ for some subset $\{v_1', \ldots, v_k'\}$ of the roots of q. But if $j \neq 1$ we have $w - av_j \notin \{u, u_2, \ldots, u_n\}$, therefore $h(v_j) \neq 0$ for all $2 \leq j \leq m$. Hence $g = (x - v)$ and so $v \in K(w)$. As $u = w + av$ we get $u \in K(w)$. Therefore, by definition, $F \subseteq K(w)$. Q.E.D.

Now we can prove the following theorem characterizing finite Galois extensions.

6 Solvability by Radicals

This is the last section of these notes and in this section we prove that an arbitrary quintic in $\mathbb{Q}[x]$ is not solvable by radicals.

Definition 6.1 *An extension F/K is called a* **radical extension** *of K if there exist elements $u_1, \ldots, u_m \in F$ such that*

1. *$F = K(u_1, \ldots, u_m)$ and*
2. *There exist positive integers $n_1, \ldots, n_m$ such that $u_1^{n_1} \in K$ and $u_i^{n_i} \in K(u_1, \ldots, u_{i-1})$ for $2 \leq i \leq m$.*

For $f \in K[x]$, the polynomial equation $f(x) = 0$ is said to be **solvable by radicals** *if there exists a radical extension F/K that contains all roots of $f(x)$.*

So to build radical extensions, we first want to examine the splitting fields for polynomials of the form $x^n - a \in K[x]$ where $n \in \mathbb{N}$ and $a \in K$. We start with the special case of examining splitting fields of $x^n - 1$.

Proposition 6.2 *Let F be the splitting field of $x^n - 1$ over a field K of characteristic zero. Then* Gal(F/K) *is abelian.*

Proof: Since K has zero characteristic, $x^n - 1$ has n distinct roots in F and it is easy to check they form a subgroup C of $F^\times = F \setminus \{0\}$. Let m be the maximal order of any element in C. Then, by the Fundamental Theorem of Finitely Generated Abelian Groups, every element of C has an order that divides m. Therefore $x^m - 1 = 0$ has at least n solutions, therefore $n \leq m$. In particular, it follows that C must be cyclic of order n.

By Theorem 2.2, Gal(F/K) must permute the elements of C. As $F = K(C)$, we have Gal(F/K) is isomorphic to a subgroup of Aut(C). But $\mathrm{Aut(C)} \cong \mathbb{Z}_\mathrm{n}^\times$ by Homework Problem I.2.15. Therefore, Gal(F/K) is abelian. Q.E.D.

We call the roots of $x^n - 1$ the **n-th roots of unity**. Any generator of the group C is called a **primitive nth root of unity**.

Theorem 6.3 *Let K be a field of characteristic zero that contains all nth roots of unity. Then for any $a \in K$ the Galois group of $x^n - a$ is cyclic and has order dividing n.*

Proof: Let u be a root of $x^n - a$ in some splitting field of $x^n - a$ over K. Let $\zeta \in K$ be a primitive nth root of unity. Then one can check that the set $\{u, \zeta u, \ldots, \zeta^{n-1}u\} \subseteq F$ is a set of n distinct roots of $x^n - a$, hence this must be a complete list. So $F = K(u)$ and any $\sigma \in \mathrm{Gal(F/K)}$ is completely determined by its value on u. Therefore we define an injective map $\phi : \mathrm{Gal(F/K)} \to \mathbb{Z}_\mathrm{n}$ given by $\phi(\sigma) = k$ if $\sigma(u) = \zeta^k u$. Then for any $\sigma, \tau \in \mathrm{Gal(F/K)}$ such that $\sigma(u) = \zeta^k u$ and $\tau(u) = \zeta^r u$ we have $\sigma\tau(u) = \sigma(\zeta^r u) = \zeta^r \sigma(u) = \zeta^{r+k} u$, hence ϕ is

a monomorphism. Therefore Gal(F/K) is isomorphic to a subgroup of $\mathbb{Z}_n$, hence Gal(F/K) must be cyclic of order dividing n. Q.E.D.

Lemma 6.4 *Let K be a characteristic zero field and let E/K be a radical extension. Then there exists an extension F/E such that F/K is a normal radical extension.*

PROOF: Let E/K be a radical extension with elements $u_1, \ldots, u_m \in E$ such that (i) $E = K(u_1, \ldots, u_m)$ and (ii) $u_i^{n_i} \in K(u_1, \ldots, u_{i-1})$ for some positive integers $n_1, \ldots, n_m$. Now let F be the splitting field of the product f of the minimal polynomials of the u_i over K $(1 \leq i \leq n)$. Now it follows from Theorem 5.7 that F/K is Galois hence a normal extension. So the proof of Part II of the Fundamental Theorem of Galois Theory tells us that in F each root of $f(x)$ has the form $\sigma(u_i)$ for some $1 \leq i \leq m$ and some $\sigma \in$ Gal(F/K). Hence for any $\sigma \in$ Gal(F/K) and any $1 \leq i \leq m$ we have $\sigma(u_i)^{n_i} \in K(\sigma(u_1), \ldots, \sigma(u_{i-1}))$. Therefore, if Gal(F/K) $= \{\sigma_1, \ldots, \sigma_k\}$ then $F = K(\{\sigma_j(u_i) | 1 \leq i \leq m, 1 \leq j \leq k\})$ is a normal radical extension of K. Q.E.D.

Finally we have the following result relating the solvability of polynomials to the solvability of the Galois group of the polynomial.

Theorem 6.5 *Let K be a field of characteristic zero and choose $f \in K[x]$ of positive degree. If $f(x) = 0$ is solvable by radicals then the Galois group of f over K is solvable.*

NOTE: The converse of this theorem is also true and a proof of the converse is given in Beachy/Blair as Theorem 8.4.6. The proof of the converse depends on Lemma 8.4.4 of Beachy/Blair.

PROOF: Let F/K be a radical extension of K that contains a splitting field E of f over K. By Lemma 6.4 we may assume F/K is normal radical extension. Let $u_1, \ldots, u_m \in F$ be such that $F = K(u_1, \ldots, u_m)$ and that there exist positive integers $n_1, \ldots, n_m$ such that $u_i^{n_i} \in K(u_1, \ldots, u_{i-1})$ for all $1 \leq i \leq m$. Let n be the least common multiple of the n_i's and let ζ be a primitive nth root of unity over K. (So $\zeta^{(n/n_i)} \in K(\zeta)$ is a primitive n_ith root of unity.) Then $F(\zeta)/K(\zeta)$ is a normal radical extension and $F(\zeta)/K$ is Galois. As E/K is Galois, it follows from Part II of the Fundamental Theorem of Galois Theory that Gal(E/K) is a factor group of Gal(F(ζ)/K). Hence, by Theorem II.7.11, if we show Gal(F(ζ)/K) is solvable then we get Gal(E/K) is also solvable.

For each $1 \leq i \leq m$, let $F_i = K(\zeta, u_1, \ldots, u_i)$. Now we will use the F_i to create a solvable series for $G =$ Gal(F(ζ)/K). Since $F_0 = K(\zeta)$ is a splitting field of the separable polynomial $x^n - 1$ over K, $K(\zeta)/K$ is Galois, hence by Part II of the Fundamental Theorem of Galois Theory $N_0 =$ Gal(F(ζ)/K(ζ)) is a normal subgroup of G and $G/N \cong$ Gal(K(ζ)/K), which is abelian by Proposition 6.2. Now, for all $1 \leq i \leq m$, F_{i-1} contains all the n_ith roots of unity and F_i is the splitting field of $x^{n_i} - (u_i)^{n_i}$, hence F_i/F_{i-1} is Galois. Therefore, by Part II of the

Fundamental Theorem, $N_i = \mathrm{Gal(F(\zeta)/F_i)}$ is a normal subgroup of $N_{i-1} = \mathrm{Gal(F(\zeta)/F_{i-1})}$ and $N_{i-1}/N_i \cong \mathrm{Gal(F_i/F_{i-1})}$. But, by Theorem 6.3, $\mathrm{Gal(F_i/F_{i-1})}$ is cyclic, hence abelian. Therefore

$$G > N_0 > N_1 > \cdots > N_m = \langle \mathrm{id_{F(\zeta)}} \rangle$$

is a solvable series. Q.E.D.

It is the contrapositive statement of Theorem 6.5 that is of most interest to us. In particular, if $f \in K[x]$ is such that its Galois group is not solvable, then $f(x) = 0$ is not solvable by radicals. We will prove this is true for any irreducible polynomial over $\mathbb{Q}$ of prime degree $p \geq 5$ that has $p-2$ real roots. We first need the following lemma.

Lemma 6.6 *Let p be a prime and let $H < S_p$. If H contains a transposition and a cycle of length p, then $H = S_p$.*

PROOF: Without loss of generality, we may assume $(1,2) \in H$. Let $\sigma \in H$ be the p-cycle. Since p is prime, we can replace σ by an appropriate power of σ, so we can assume $\sigma = (1, 2, a_3, \ldots, a_p)$. Now, by renaming elements, we can assume $\sigma = (1, 2, 3, \ldots, p)$. As H is a subgroup, $\theta = (2, 3, \ldots, p) = (1,2)(1, 2, 3, \ldots, p) \in H$. Then we check $\theta^k(1,2)\theta^{-k} = (1, k+1)$ for all $1 \leq k \leq p-1$. Hence $(1,k) \in H$ for $k = 2, \ldots, p$. Finally, for any $k_1, k_2 \neq 1$, $(1,k_1)(1,k_2)(1,k_1) = (k_1, k_2) \in H$, hence all transpositions are in H. Now by Corollary I.6.5, $H = S_p$. Q.E.D.

Now for the finale.

Theorem 6.7 *If p is prime and $f \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$ of degree p having $p-2$ real roots, then the Galois group of f over $\mathbb{Q}$ is isomorphic to S_p. Therefore, if $p \geq 5$, $f(x) = 0$ is not solvable by radicals.*

PROOF: Let $F \subseteq \mathbb{C}$ be a splitting field of f over $\mathbb{Q}$. As $F = \mathbb{Q}(r_1, \ldots, r_p)$ where $r_1, \ldots, r_p \in \mathbb{C}$ are the distinct roots of f, there exists an injective homomorphism $\phi : \mathrm{Gal(F/\mathbb{Q})} \to \mathrm{S_p}$ since by Theorem 2.2 $\mathrm{Gal(F/\mathbb{Q})}$ must permute the roots of f. (This is an exercise using Theorem 2.2.) Identify $\mathrm{Gal(F/\mathbb{Q})}$ with its image in S_p under ϕ. Now $[\mathbb{Q}(r_1) : \mathbb{Q}] = p$ by Theorem 1.6 and since $F/\mathbb{Q}$ is Galois, $|\mathrm{Gal(F/\mathbb{Q})}| = [\mathrm{F} : \mathbb{Q}] = [\mathrm{F} : \mathbb{Q}(\mathrm{r_1})][\mathbb{Q}(\mathrm{r_1}) : \mathbb{Q}]$, so p divides $|\mathrm{Gal(F/\mathbb{Q})}|$. Now by Cauchy's Theorem, there exists an element of order p in $\mathrm{Gal(F/\mathbb{Q})}$. But the only elements of order p in S_p are p-cycles, so $\mathrm{Gal(F/\mathbb{Q})}$ contains a p-cycle. Also, complex conjugation restricted to F is a field automorphism that exchanges the two complex roots and leaves all other roots fixed. Therefore, $\mathrm{Gal(F/\mathbb{Q})}$ also contains a transposition. So by Lemma 6.6, $\mathrm{Gal(F/\mathbb{Q})} = \mathrm{S_p}$.

If $p \geq 5$, we have shown that S_p is not solvable (since A_p is nonabelian and simple), hence $\mathrm{Gal(F/\mathbb{Q})}$ is not a solvable group. So by Theorem 6.5, $f(x) = 0$ is not solvable by radicals.

Q.E.D.

We point out Abel's result (Proposition V.9.8 of Hungerford) that says that over $\mathbb{Q}$ that the general equation of degree n is solvable by radicals only if $n \leq 4$.

We close with the standard example of a non-solvable quintic equation.

Example. Consider the equation $x^5 - 4x + 2 = 0$ over $\mathbb{Q}$. One can verify by looking at the graph that $f(x) = x^5 - 4x + 2$ has three real roots. By Eisenstein's Criterion (Theorem 4.3.6 of Beachy/Blair), $f(x)$ is irreducible over $\mathbb{Q}$. Therefore, by Theorem 6.7, the Galois group of $f(x)$ over $\mathbb{Q}$ is isomorphic to S_5 and hence $x^5 - 4x + 2 = 0$ is not solvable by radicals.