GALOIS THEORY NOTES

JAMES MARSHALL REBER

Contents

The goal is to build up to Galois theory using Jacobson [1] and Artin [2], following Cogdell's notes [3].

1. Preliminaries

1.1. Extension Fields.

Definition. Let E, F be fields. If F is a subfield of E, i.e. $F \subset E$ and F is closed under the operations, then we call E an extension of F. We will (maybe poorly) denote E being an extension of F by $E \subset F$. We will also sometimes write E/F for E being an extension of F.

We remark that if E/F is an arbitrary extension, we can view E as a vector space over F. The action will simply be multiplication; i.e. if $x \in E$, $r \in F$, then $r \cdot x = rx$ (the usual multiplication as a field). The other axioms for a vector space follow just as easily. As a result, we'll sometimes ambiguously write E/F for a field extension and as a way of denoting the vector space E over F.

Definition. Let E/F be a field extension. We define the degree of the extension, denoted by $(E : F)$, to be the dimension of E as a vector space over F. That is,

$$(E : F) = \dim_F(E)$$

is the degree of E over F.

There is a multiplicativity that comes with degrees of field extensions.

Theorem 1. Let $F \subset E \subset K$ be fields. Then $(K : F)$ is finite iff $(K : E)$ and $(E : F)$ are finite, and moreover we have that

$$(K : F) = (K : E)(E : F).$$

Proof. ($\implies$): Assume first that $(K : F)$ is finite. Furthermore, since $E \subset K$, we can view E/F as a subspace of K/F. Consequently, $(E : F) \leq (K : F) < \infty$, so $(E : F)$ is finite.

Next, we wish to show that $(K : E)$ is finite as well. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for K/F. Then every element $\beta \in K$ can be written as

$$\beta = \sum_{j=1}^{n} a_j \alpha_j,$$

where $a_j \in F$. Notice that, in particular, the $\alpha_j \in E$ as well, so we have that $\{\alpha_1, \ldots, \alpha_n\}$ span K/E as well. Consequently, we get that $(K : E) \leq (K : F) < \infty$. So they're both finite.

($\impliedby$) : Assume $(K : E)$ and $(E : F)$ are both finite. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for E/F, $\{\beta_1, \ldots, \beta_m\}$ be a basis for K/E. We wish to show that we can use these to find a finite basis for K/F. Let $\beta \in K$ be arbitrary, then we have

$$\beta = \sum_{j=1}^{m} a_j \beta_j,$$

where $a_j \in E$. Notice that for each j, we have

$$a_j = \sum_{i=1}^{n} b_{i,j} \alpha_i,$$

where $b_{i,j} \in F$. Hence, substituting this in, we have

$$\beta = \sum_{j=1}^{m} \sum_{i=1}^{n} b_{i,j} \alpha_i \beta_j.$$

In other words, we have $\{\alpha_i \beta_j\}_{i=1,j=1}^{i=n,j=m}$ form a spanning set for K/F, giving us that $(K : F) < \infty$ as well.

Finally, we need to show the moreover clause. Suggestively, we should check that $\{\alpha_i\beta_j\}_{i=1,j=1}^{i=n,j=m}$ form a basis for K/F. If we have this, then $(K:F) = (K:E)(E:F)$, as desired. Since it's a spanning set apriori, it suffices to show that it's linearly independent. Assume that

$$\sum_{j=1}^{m}\sum_{i=1}^{n} b_{i,j}\alpha_i\beta_j = 0.$$

Notice that, since the β_j are a basis, this implies that for each j,

$$\sum_{i=1}^{n} b_{i,j}\alpha_i = 0,$$

and since the α_i form a basis, we get that for each i $b_{i,j} = 0$. Hence, for every (i,j), we have $b_{i,j} = 0$, and so we must have that the set is linearly independent. That is, it's a basis. □

Corollary 1. If $F \subset F_1 \subset \cdots \subset F_n$ is a chain of extensions of fields, then

$$(F_n : F) = (F_n : F_{n-1}) \cdots (F_1 : F).$$

Proof. This is a simple induction exercise. We've shown it for the case $n = 2$ in the prior theorem. Assume it holds for $n-1$. Then for the case of n, we have

$$(F_n : F) = (F_n : F_{n-1})(F_{n-1} : F)$$

by the $n = 2$ case. Applying the induction hypothesis gives the result. □

We introduce some more notation. Let E/F be an extension of fields, $S \subset E$ a subset of the elements of E. Then we denote by $F[S]$ the subring of E generated by F and S and $F(S)$ the subfield generated by F and S [Parentheses will, in general, have a connotation of inverses].

Let $S = \{\alpha_1, \ldots, \alpha_n\}$ be finite. Consider the map $\varphi : F[x_1, \ldots, x_n] \to E$, where $\varphi(p(x_1, \ldots, x_n)) = p(\alpha_1, \ldots, \alpha_n)$; that is, φ is the evaluation map. Notice, then, that $F[S] = \varphi(F[x_1, \ldots, x_n])$; i.e. $F[S] = \mathrm{Im}(\varphi)$. This gives us a more concrete way of viewing this subring. Analogously, if $\phi : F(x_1, \ldots, x_n) \to E$ is also given by evaluation, then we can view $F(S) = \mathrm{Im}(\phi)$.

1.2. **(Optional) Polynomials.** While a little silly, we'll diverge from the notes [3] to recall some facts on polynomials. This will hopefully make the next section a little easier to digest. This is Artin II B. [2].

Recall that an expression of the form $a_n x^n + \cdots + a_0 = p(x)$ is a polynomial of degree n as long as the $a_i \in F$, a field, and $a_n \neq 0$. Addition of polynomials is done in the obvious fashion; if $n \leq m$, then

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i = \sum_{k=0}^{m} (a_i + b_i) x^i,$$

where if $i > n$ then we set $a_i = 0$. Multiplication is done via a convolution fashion; that is,

$$\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{k=0} c_k x^k,$$

where

$$\sum_{i+j=k} a_i b_j = c_k.$$

Let $\deg : F[x] \to \mathbb{Z}_{\geq 0} \cup \{-\infty\}$ be the function which evaluates the degree of a polynomial. Notice that $\deg(p(x) + q(x)) \leq \max\{\deg(p(x)), \deg(q(x))\}$, and $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$, and we assign to 0 the degree $-\infty$ (hence why we added it on).

Recall that a polynomial is reducible in F if it is equal to the product of two polynomials in F, each of degree at least one. Polynomials which are not reducible are said to be irreducible.

If $p(x) = q(x)h(x)$, then we say that $q(x)$ divides $p(x)$ and that $q(x)$ is a factor of $p(x)$. By the observation of degree above, we have $\deg(q(x)) \leq \deg(p(x))$ if it is a factor of $p(x)$. Note as well we can always represent polynomials as a product of finitely many irreducible polynomials.

Recall as well we have the division algorithm for polynomials; for any two polynomials $p(x)$ and $q(x)$, there exists a $g(x)$ and an $r(x)$ so that

$$p(x) = g(x)q(x) + r(x),$$

and such that $\deg(r(x)) < \deg(g(x))$. We have that $r(x)$ is referred to as the remainder. A consequence of this over fields is that if $a \in F$ is so that $p(a) = 0$, then $p(x) = (x - a)g(x)$ for some $g(x)$. First, notice that the division algorithm tells us that $p(x) = (x - a)g(x) + r(x)$. Viewing $g(x)$ as the divisor, notice that this forces the remainder to have degree strictly less than 1; i.e., it must be a constant. So we have $p(x) = (x - a)g(x) + r$. Substituting in a, we have $0 = p(a) = (a - a)g(a) + r = r$. So $r = 0$, and therefore $p(x) = (x - a)g(x)$. Note that a consequence of this is that a polynomial cannot have more roots in the field than its degree.

The following lemma tells us the uniqueness of irreducible polynomials up to constants.

Lemma 1. If $p(x)$ is an irreducible polynomial of degree n in F, then there do not exist two polynomials each of degree less than n in F whose product is divisible by $p(x)$.

Proof. We proceed by contradiction. Assume $h(x), q(x)$ are such that $p(x) \mid h(x)q(x)$,

$$\max\{\deg(q(x)), \deg(h(x))\} < \deg(p(x)) = n.$$

Among all pairs $h(x)$ and $q(x)$, let $h(x)$ be the one with minimal degree. Since $p(x) \mid h(x)q(x)$, we have a polynomial $k(x)$ so that

$$p(x)k(x) = h(x)q(x).$$

We now apply the division algorithm; we have

$$p(x) = d(x)h(x) + r(x),$$

where $\deg(r(x)) < \deg(h(x))$. Since $p(x)$ is irreducible, we get as well that $r(x) \neq 0$. The goal, then, is to show that $r(x)$ is paired with a polynomial so that $f(x)$ divides their product; in doing so, we will have a contradiction, since $h(x)$ was assumed to have the smallest degree.

Multiplying by $q(x)$, we have

$$q(x)p(x) = q(x)d(x)h(x) + q(x)r(x) = k(x)p(x)d(x) + q(x)r(x).$$

Subtracting, we get then that

$$q(x)r(x) = p(x)q(x) - k(x)p(x)d(x) = p(x)\left[q(x) - k(x)d(x)\right].$$

In other words, $p(x) \mid r(x)q(x)$, but $\deg(r(x)) < \deg(h(x))$, which gives a contradiction. □

1.3. **Algebraic Elements.**

Definition. If E/F is an extension of fields, $\alpha \in E$, then we say that α is algebraic if it is the root of a non-zero polynomial $p(x) \in F[x]$. In other words, α is algebraic if there exists $p(x) \in F[x]$, $p(x) \neq 0$, where $p(\alpha) = 0$.

Consider now the map $\varphi_\alpha : F[x] \to E$ where $\varphi_\alpha(p(x)) = p(\alpha)$; that is, the evaluation map. If $\alpha \in E$ is algebraic, then we see that there exists a polynomial $p(x)$ where $\varphi_\alpha(p(x)) = p(\alpha) = 0$. Thus, the map φ_α has non-zero kernel iff α is algebraic. Recall that the kernel, $\mathrm{Ker}(\varphi_\alpha) = K \subset F[x]$, forms an ideal. Recall as well that if F is afield, then the ring $F[x]$ is a principle ideal domain, so we have $K = (p_\alpha(x))$ for some polynomial $p_\alpha(x) \in F[x]$. Note that we can make $p_\alpha(x)$ monic (by dividing out the leading coefficient, since we're in a field) and we have $p_\alpha(x)$ is irreducible (we get

a contradiction otherwise by the division algorithm). We call $p_\alpha(x)$ the minimal polynomial. We formalize the last paragraph in the next definition.

Definition. If E/F is a field extension, the minimal polynomial for $\alpha \in E$ in $F[x]$ is the monic polynomial which generates the kernel of $\varphi_\alpha : F[x] \to E$ defined by $\varphi_\alpha(p(x)) = p(\alpha)$.

Note that the minimal polynomial is the polynomial of $f(x)$ of least degree so that $f(\alpha) = 0$. This is a consequence of the fact that the $p_\alpha(x)$ generates the kernel of the map φ_α; if $f(x)$ is a polynomial of degree smaller, then p_α would divide it, giving us a contradiction.

Minimal polynomials are useful for looking at field extensions.

Theorem 2. Let E/F be an extension of fields. Then $\alpha \in E$ is algebraic over F if and only if $(F(\alpha) : F) < \infty$.

Proof. ($\implies$) : Assume α is algebraic, and let

$$p_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$$

be its minimal polynomial. Note that we have $F[\alpha] \cong F[x]/(p_\alpha(x))$, and since $p_\alpha(x)$ is irreducible, we get $F[\alpha] = F(\alpha)$. The goal, then, is to find a basis for $F(\alpha)$ over F. Note that for all $g(x) \in F[x]$, the division algorithm gives us that

$$g(x) = q(x)p_\alpha(x) + r(x),$$

where $\deg(r(x)) < \deg(p_\alpha(x)) =: n$. Evaluating $g(\alpha) = \varphi_\alpha(g(x))$, then, we have

$$g(\alpha) = q(\alpha)p_\alpha(\alpha) + r(\alpha) = r(\alpha).$$

That is,

$$g(\alpha) = a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0.$$

Thus, the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ form a spanning set for $F(\alpha)$. We check now that this forms a basis. Assume now that we have

$$a_0 + \cdots + a_{n-1}\alpha^{n-1} = 0,$$

then this implies that we can form a polynomial

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$$

where $\varphi_\alpha(f(x)) = f(\alpha) = 0$. This is a contradiction if there is an $a_i \neq 0$ for some i, since we have that $p_\alpha(x)$ is the minimal polynomial and this would give us a polynomial of degree smaller.

($\impliedby$): We prove this by contrapositive. Assume that α is not algebraic. Then there is no polynomial $p(x) \in F[x]$ so that $p(\alpha) = 0$. Recall that an infinite set of elements is linearly independent if every finite subset of it is linearly independent. Examining the set $\{\alpha^i\}_{i\geq 0}$, we see that every finite subset must be linearly independent, since otherwise we would have a polynomial which evaluates to 0 at α, contradicting the fact that α is not algebraic. Thus, this forms an infinite linearly independent set, and so $(F(\alpha) : F) = \infty$. □

Notice that in the proof of the prior theorem, we've established the following result.

Corollary 2. If $\alpha \in E$ is algebraic over F, then we have that

$$(F(\alpha) : F) = \deg(p_1(x)).$$

Proof. In the prior proof, we had that if α is algebraic, then $\{1, \ldots, \alpha^{n-1}\}$ forms a basis for $F(\alpha)$ over F, where $n = \deg(p_1(x))$. This gives the desired result. □

Definition. If E/F is a field extension, an element $\alpha \in E$ is called transcendental if it is not algebraic. In other words, there does not exist a $p(x) \in F[x]$ so that $p(\alpha) = 0$.

The goal now is to flip this last theorem. That is, we wish to take $p(x) \in F[x]$ and find a field extension E/F where $p(x)$ has a root in E. We can do this by a theorem from Kronecker.

Theorem 3 (Kronecker)**.** If $p(x) \in F[x]$ is a polynomial of degree greater than or equal to 1, then there exists an extension E/F in which $p(x)$ has a root.

Proof. Like before, we assume $p(x)$ is monic; we can do so by dividing out by the leading coefficient. Applying the division algorithm a finite number of times, we can write

$$p(x) = p_1(x) \cdots p_k(x),$$

where $p_i(x)$ is monic and irreducible in $F[x]$. It suffices, then, to construct an extension E/F in which $p_1(x)$ has a root (we can do this same process for all $p_i(x)$, $1 \leq i \leq k$). We remark that this is easy if $p_1(x) = x - a$; that is, if $p_1(x)$ has degree 1. In this case, a is the root, so our field extension is just F itself.

Assume now that $\deg(p_1(x)) \geq 2$. As suggested in the proof of the last theorem, let's try examining $E = F[x]/(p_1(x))$. Recall that irreducible elements form maximal ideals, so $(p_1(x))$ is maximal, and hence E is a field. Note as well that $F \subset E$, so E constitutes a field extension. It suffices to then show that E contains a root for $p_1(x)$.

Let

$$\alpha = x + (p_1(x)) \in E.$$

Then we see that $E = F(\alpha) = F[x]/(p_1(x))$, and we observe that $p_1(\alpha) = 0$. Thus, we have that E/F is an extension which contains a root of $p_1(x)$, and hence a root of $p(x)$. □

We remark that, using **Corollary 2**, we have that the extension constructed in **Theorem 3** is such that

$$(E : F) = \deg(p_1(x)) \leq \deg(p(x)).$$

A consequence of Kronecker is the following theorem.

Theorem 4. Let $\sigma : F \to F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ be irreducible, $p'(x) = \sigma(p(x)) \in F'[x]$. Then if $E = F(\beta)$, where $p(\beta) = 0$, and if $E' = F'(\beta')$, where $p'(\beta') = 0$, then σ can be extended to an isomorphism $\sigma : E \to E'$.

Proof. We first remark the following lemma.

Lemma 2. If $p(x) \in F[x]$ is irreducible, $\sigma : F \to F'$ is an isomorphism of fields, then $\sigma(p(x)) = p'(x)$ is also irreducible, where $\sigma : F[x] \to F'[x]$ is a ring isomorphism defined by $\sigma(x) = x$ and extending it linearly.

Proof. Assume for contradiction $p'(x)$ were not irreducible. Then there exists $q(x)$, $h(x)$ with degrees greater than or equal to 1 such that $p'(x) = q(x)h(x)$. That is, we have

$$p'(x) = \left(\sum_{j=0}^{n} a_j x^j\right)\left(\sum_{i=0}^{m} b_j x^j\right).$$

Applying σ^{-1}, we get

$$\sigma^{-1}(p'(x)) = p(x) = \sigma^{-1}\left(\left(\sum_{j=0}^{n} a_j x^j\right)\left(\sum_{i=0}^{m} b_j x^j\right)\right) = \left(\sum_{j=0}^{n} \sigma^{-1}(a_j) x^j\right)\left(\sum_{i=0}^{m} \sigma^{-1}(b_j) x^j\right).$$

This, however, contradicts the fact that $p(x)$ was irreducible. Hence, we must have $p'(x)$ is also irreducible. □

From the proof of Kronecker (**Theorem 3**), we remark that we have an isomorphism

$$\theta : F(\beta) \to F[x]/(p(x)),$$

defined by $\beta \mapsto x + (p(x))$. Using the idea in **Lemma 2**, we get an isomorphism

$$\sigma : F[x]/(p(x)) \to F'[x]/(p'(x)).$$

Finally, we note that we have an isomorphism

$$\theta'^{-1} : F'[x]/(p'(x)) \to F'(\beta')$$

defined by $x + (p'(x)) \mapsto \beta'$. Combining these together, we can extend σ to $F(\beta) \to F'(\beta')$ by following $\theta'^{-1}\sigma\theta$. □

1.4. **Splitting Fields.**

Definition. Let F be a field, $p(x) \in F[x]$ monic. An extension E/F is called a splitting field of $p(x)$ over F if two conditions are satisfied:

(1) $p(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ in $E[x]$ (the polynomial splits),
(2) $E = F(\alpha_1, \ldots, \alpha_n)$ (it is the minimal extension for which the polynomial splits).

There is one nice observation we can make on splitting fields.

Lemma 3. If E is the splitting field for a field F, then $(E : F) < \infty$.

Proof. We observed earlier that the number of roots of a polynomial cannot exceed the degree. Let $p(x)$ be a polynomial of degree n. By Kronecker, we can find a field extension $F(\alpha_1)/F$ where $p(\alpha_1) = 0$. Repeatedly applying it, we have $E = F(\alpha_1, \ldots, \alpha_n)/F(\alpha_1, \ldots, \alpha_{n-1})/\ldots/F$, and furthermore we see that $(F(\alpha_1, \ldots, \alpha_j) : F(\alpha_1, \ldots, \alpha_{j-1})) < \infty$ for all $1 \leq j \leq n$. By **Theorem 1**, we have

$$(E : F) = \prod_{j=1}^{n} (F(\alpha_1, \ldots, \alpha_j) : F(\alpha_1, \ldots, \alpha_{j-1})) < \infty.$$

□

Naturally, we need to explore whether or not splitting fields exist for individual polynomials. The answer is yes.

Theorem 5. If $p(x) \in F[x]$ is a monic polynomial with $\deg(p) \geq 1$, then there exists a splitting field E of $p(x)$.

Proof. Factor the polynomial into irreducible factors; that is, we have $p(x) = p_1(x) \cdots p_r(x)$, with $p_i(x) \in F[x]$ irreducible for $1 \leq i \leq r$. Note that $r \leq n = \deg(p(x))$. We do induction on $n - r$. First, if $n - r = 0$, then this means that the $p_i(x)$ are all linear factors, and so $p(x)$ splits already in $F[x]$. Hence, a splitting field exists. If $n - r > 0$, then $p_i(x)$ has degree bigger than 1 for some i. Assume without loss of generality that $i = 1$ (this is just for notational convenience). By Kronecker, we construct $K = F(\alpha_1)$, where $p_1(\alpha_1) = 0$. Notice that $p(x) \in F[x] \subset K[x]$, and note that in $K[x]$, we have $p_1(x) = (x - \alpha_1)g_1(x)$. Thus, factoring $p(x)$ in $K[x]$, we see that the number of irreducible factors must strictly increase. If we have k irreducible factors in $K[x]$, then we note that $k > r$ (strictly), and hence $n - k < n - r$. Applying the induction hypothesis, we can find a splitting field E/K, where

$$p(x) = (x - \alpha_1) \cdots (x - \alpha_n) \text{ in } E[x].$$

Thus, adjoining α_1, we have $E = K(\alpha_2, \ldots, \alpha_n) = F(\alpha_1)(\alpha_2, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_n)$, so E is a splitting field of p over F. □

1.5. **Uniqueness of Splitting Fields.** Now that we have a splitting field for our polynomial, the next question to ask is whether it is unique (up to isomorphism, of course; we could just rearrange variables to keep getting other splitting fields). A preliminary theorem will be extending isomorphisms of fields to isomorphisms of splitting fields.

Theorem 6. Let $\sigma : F \to F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ and $p'(x) = \sigma(p(x)) \in F'[x]$. Let E/F be a splitting field of $p(x)$ over F, E'/F' a splitting field of $p'(x)$ over F'. Then σ can be extended to an isomorphism $\sigma; : E \to E'$.

Note that as a corollary, we have the following.

Corollary 3. If $p(x) \in F[x]$, then any two splitting fields of $p(x)$ are isomorphic.

Proof. Take $\sigma : F \to F$ to be the identity and apply the theorem. □

We now prove the theorem.

Proof. Let E be a splitting field of $p(x)$ over F. If $f(x) \in F[x]$ is an irreducible factor of $p(x)$, then E contains a root of $f(x)$. We then prove this based on the number of roots of $p(x)$ which do *not* lie in F. First, if all of the roots of $p(x)$ lie in F, so

$$p(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

in $F[x]$, then

$$p'(x) = (x - \alpha_1') \cdots (x - \alpha_n')$$

in $F'[x]$, where $\alpha_i' = \sigma(\alpha_i) \in F'$. In this case, σ' is just σ, and we're done.

Now, we induct on the number of roots which do not lie in F. Suppose $k \geq 1$. Factor $p(x)$ into it's irreducible factors, i.e. we examine

$$p(x) = f_1(x) \cdots f_m(x)$$

in $F[x]$, where each $f_i(x)$ is irreducible. Notice that there must be some $f_i(x)$ so that $\deg(f_i(x)) > 1$, since otherwise $p(x)$ splits. Assume for simplicity this is $f_1(x)$. Hence, $\deg(f_1(x)) > 1$. Applying σ, we get

$$p'(x) = f_1'(x) \cdots f_m'(x)$$

in $F'[x]$ is the decomposition of $p'(x) = \sigma(p(x))$ into irreducibles in $F'[x]$, where we have $f_i'(x) = \sigma(f_i(x))$.

By **Theorem 4**, we have that if α is a root of $f_1(x)$ in E and α' is a root of $f_1'(x)$ in E', then σ extends to an isomorphism, say $\sigma_1 : F(\alpha) \to F'(\alpha')$. Now, note we have $F \subset F(\alpha) \subset E$, $F' \subset F'(\alpha') \subset E'$, so we have that E is a splitting field of $p(x)$ over $F(\alpha)$ and E' is a splitting field of $p'(x)$ over $F'(\alpha')$. We've now reduced the number of roots, so we can hit it with the induction hypothesis to extend σ_1 to an isomorphism $\sigma' : E \to E'$ over $\sigma_1 : F(\alpha) \to F'(\alpha')$, and σ_1 extends σ, so σ' extends σ. Thus, we have the desired result. □

1.6. **Group Characters.** Let G be a group written multiplicatively. The goal is to take $G = E^\times$ to be the multiplicative group of a field.

Definition. Let F be a field. A homomorphism

$$\sigma : G \to F$$

is called a character of G in F.

As an aside, this is a 1-dimensional representation of G with image not necessarily in $\mathcal{C}$, but rather in the field F. Since elements in G have inverses, we note that the image of σ must lie in $F^\times$; otherwise, if $\sigma(a) = 0$ for some a, we get $\sigma(x) = 0$ for all $x \in G$. To see this, we apply a^{-1} to get

$$\sigma(1) = \sigma(aa^{-1}) = \sigma(a)\sigma(a^{-1}) = 0,$$

so for all $x \in G$ we have

$$\sigma(x) = \sigma(x1) = \sigma(x)\sigma(1) = 0.$$

In practice, we will consider the embeddings $\sigma_i : E \hookrightarrow E'$ restricted to $E^\times$.

Definition. If $\sigma_1, \ldots, \sigma_n : G \to F$ are characters in F, they are called independent (over F) if any relation

$$a_1\sigma_1(x) + \cdots + a_n\sigma_n(x) = 0 \ \forall x \in G$$

with coefficients $a_1, \ldots, a_n \in F$ is trivial; i.e.,

$$a_1\sigma_1(x) + \cdots + a_n\sigma_n(x) = 0 \ \forall x \in G$$

implies $a_1 = \cdots = a_n = 0$.

One should note this is similar to linear independence for a vector space.

It turns out we have a powerful result telling us that characters are independent, so long as they are distinct.

Theorem 7 (Dedekind's Independence of Characters)**.** If G is a group and $\sigma_1, \ldots, \sigma_n$ are n distinct characters of G with values in a field F, then $\sigma_1, \ldots, \sigma_n$ are independent over F.

Proof. As usual, we induct. For the case $n = 1$, the result should follow. If we have the relation $a_1\sigma(x) = 0$ for all $x \in G$, then choosing the identity, we have $a_1\sigma(1) = a_1 = 0$ [Note: This follows by our earlier remark since $\sigma : G \to F^\times$ is a group homomorphism.]

It turns out the case $n = 2$ will be of most use to us. Suppose that we have the non-trivial relation

$$a_1\sigma_1(x) + a_2\sigma_2(x) = 0$$

for all $x \in G$. Notice that we may assume $a_1, a_2 \neq 0$, since otherwise this reduces to the $n = 1$ case, and we have a contradiction immediately. By assumption, σ_1 and σ_2 are distinct, so $\sigma_1(a) \neq \sigma_2(a)$ for some $a \in G$. Dividing out by, say, a_2, we have

$$\frac{a_1}{a_2}\sigma_1(x) + \sigma_2(x) = 0 \ \forall x \in G. \tag{1}$$

Substitute in ax, where $x \in G$ is arbitrary. Then we have

$$\frac{a_1}{a_2}\sigma_1(a)\sigma_1(x) + \sigma_2(a)\sigma_2(x) = 0.$$

Divide out by $\sigma_2(a)$ to get

$$\frac{a_1\sigma_1(a)}{a_2\sigma_2(a)}\sigma_1(x) + \sigma_2(x) = 0 \tag{2}$$

for all $x \in G$. Subtracting equation (2) from equation (1), we are left with

$$\left[\frac{a_1}{a_2}\left(1 - \frac{\sigma_1(a)}{\sigma_2(a)}\right)\right]\sigma_1(x) = 0 \ \forall x \in G.$$

However, by assumption, $a_1, a_2, \sigma_1(a), \sigma_2(a) \neq 0$, and $1 - \sigma_1(a)/\sigma_2(a) \neq 0$, so we have a non-trivial relation, contradicting our $n = 1$ case.

The case $n > 2$ follows similarly. Assume the result holds for $n-1$. Assume as well that we have a non-trivial relation

$$a_1\sigma_1(x) + \cdots + a_n\sigma_n(x) = 0 \ \forall x \in G.$$

Like before, we may assume $a_i \neq 0$ for all $1 \leq i \leq n$, since otherwise this reduces to the $n-1$ case, and we immediately get a contradiction. Dividing out by a_n and letting $b_i = a_i/a_n$ for $1 \leq i \leq n-1$, we have

$$b_1\sigma_1(x) + \cdots + \sigma_n(x) = 0 \ \forall x \in G. \tag{3}$$

Like in the $n = 2$ case, we use the fact that these are distinct. Notice that there exists an $a \in G$ so that $\sigma_1(a) \neq \sigma_n(a)$. Substituting ax into the equation, we get

$$b_1\sigma_1(a)\sigma_1(x) + \cdots + \sigma_n(a)\sigma_n(x) = 0 \ \forall x \in G.$$

Dividing out by $\sigma_a(x)$, we are left with

$$b_1\frac{\sigma_1(a)}{\sigma_n(a)}\sigma_1(x) + \cdots + \sigma_n(x) = 0 \ \forall x \in G. \tag{4}$$

Substracting equation (4) from (3), we have

$$b_1\left(1 - \frac{\sigma_1(a)}{\sigma_n(a)}\right)\sigma_1(x) + \cdots + b_{n-1}\left(1 - \frac{\sigma_{n-1}(a)}{\sigma_n(a)}\right)\sigma_{n-1}(x) = 0.$$

We note that

$$b_1\left(1 - \frac{\sigma_1(a)}{\sigma_n(a)}\right) \neq 0,$$

so we have a non-trivial relation among the $\sigma_1, \ldots, \sigma_{n-1}$, contradicting the induction hypothesis. Thus, it holds for all n. □

Corollary 4. If E and E' are two fields and

$$\sigma_1, \ldots, \sigma_n : E \hookrightarrow E'$$

are distinct field embeddings, then $\sigma_1, \ldots, \sigma_n$ are independent over E', i.e.,

$$a_1'\sigma_1(x) + \cdots + a_n'\sigma_n(x) \neq 0$$

for $a_1', \ldots, a_n' \in E'$, not all 0, and all $x \in E^\times$.

Proof. Take $G = E^\times$. Then $\sigma_1, \ldots, \sigma_n$ are all E' valued characters of G, and hence independent over E'. □

1.7. **Fixed Fields.**

Definition. Let $\sigma_1, \ldots, \sigma_n : E \hookrightarrow E'$ be distinct embeddings of fields. An element $\alpha \in E$ is called a fixed point of the σ_i if we have

$$\sigma_1(\alpha) = \cdots = \sigma_n(\alpha).$$

The idea behind fixed points is that if the σ_i are automorphisms and σ_1 is the identity, then $\sigma_1(x) = x$ and we have $\sigma_i(x) = x$ for $1 < i \leq n$. That is, this is an honest fixed point of the set of automorphisms.

Lemma 4. Let $\sigma_1, \ldots, \sigma_n : E \hookrightarrow E'$ be distinct field embeddings. Let F be the set of fixed points of $\sigma_1, \ldots, \sigma_n$. Then F is a subfield of E.

Remark. We call F the fixed field of $\sigma_1, \ldots, \sigma_n$.

Proof. First, since these are automorphisms, we see that $\sigma_i(0) = 0$ $\sigma_i(1) = 1$ for $1 \leq i \leq n$. Thus, $0, 1 \in F$. It suffices to show pairwise equality, so let's compare σ_i to σ_1. Then if $a, b \in F$, we see that

$$\sigma_i(a-b) = \sigma_i(a) - \sigma_i(b) = \sigma_1(a) - \sigma_1(b) = \sigma_1(a-b),$$

so

$$\sigma_1(a-b) = \cdots = \sigma_n(a-b),$$

and so $a - b \in F$. Thus, $(F, +, 0) \subset (E, +, 0)$ is a subgroup. Next, consider $a, b \neq 0$. Then we see that

$$\sigma_i(ab^{-1}) = \sigma_i(a)\sigma_i(b)^{-1} = \sigma_1(a)\sigma_1(b)^{-1} = \sigma_1(ab^{-1}),$$

and so we have

$$\sigma_1(ab^{-1}) = \cdots = \sigma_n(ab^{-1}),$$

so $(F^\times, \cdot, 1) \subset (E^\times, \cdot, 1)$ is a subgroup (recall that for a field F, $F^\times$ is the collection of elements which are non-zero; in general, $F^\times$ is the collection of units for F). Since $(F, +, 0)$ is a group, $(F^\times, \cdot, 1)$ is a group, we get that F is a field. □

Remark. Notice that if there is a single σ_1, we trivially that $F = E$, since $\sigma_1(x) = \sigma_1(x)$ for all $x \in E$.

From the proof above, we see that $F \leq E$ is a subfield. As a result, we can look at the extension E/F. We can't exactly determine the degree of this extension, however we can get a lower bound.

Theorem 8. If $\sigma_1, \ldots, \sigma_n : E \hookrightarrow E'$ are distinct, F the fixed field of $\sigma_1, \ldots, \sigma_n$, then $(E : F) \geq n$.

Proof. Suppose for contradiction that $(E : F) = r < n$. Then we have a basis of E/F given by $\omega_1, \ldots, \omega_r$. The goal is to contradict Dedekind's Independence of characters (**Theorem** 7; since these are distinct, we must have that they are independent over F (the fixed field) with regards to the multiplicative groups. We will find a non-trivial relation among them.

We build the system of equations

$$\begin{aligned} \sigma_1(\omega_1)x_1 + \cdots + \sigma_1(\omega_1)x_n &= 0 \\ &\cdots \\ \sigma_1(\omega_r)x_1 + \cdots + \sigma_n(\omega_r)x_n &= 0. \end{aligned}$$

This system has coefficients $\sigma_i(\omega_j) \in E'$. Since we have that $r < n$, we see that there is a non-zero solution; that is, we have $\beta_i \in E'$, $1 \leq i \leq n$, where not all of the β_i are zero. Substituting this in, then, we get

$$\begin{aligned} \sigma_1(\omega_1)\beta_1 + \cdots + \sigma_1(\omega_1)\beta_n &= 0 \\ &\cdots \\ \sigma_1(\omega_r)\beta_1 + \cdots + \sigma_n(\omega_r)\beta_n &= 0. \end{aligned}$$

Let $y \in E$ be arbitrary. Since the ω_i form a basis, we have that

$$y = \sum_1^r a_k\omega_k.$$

Hence,

$$\begin{aligned} &\sigma_1(y)\beta_1 + \cdots + \sigma_n(y)\beta_n \\ &= \sigma_1\left(\sum_1^r a_k\omega_k\right)\beta_1 + \cdots + \sigma_n\left(\sum_1^r a_k\omega_k\right)\beta_n \\ &= \sigma(a_1)\left[\sigma_1(\omega_1)\beta_1 + \cdots + \sigma_n(\omega_1)\beta_n\right] + \cdots + \sigma(a_r)\left[\sigma_1(\omega_r)\beta_1 + \cdots + \sigma_n(\omega_r)\beta_n\right] \\ &= \sigma(a_1)(0) + \cdots + \sigma(a_r)(0) = 0, \end{aligned}$$

where the last equality comes from the observation above. The choice of y was arbitrary, so we have that for all $y \in E$, $\sigma_1(y)\beta_1 + \cdots + \sigma_n(y)\beta_n = 0$; this contradicts Dedekind, since it in particular holds for all $y \in E^\times$, and so we cannot have $(E : F) < n$. Consequently, $(E : F) \geq n$. □

We remark that the bound is independent of the choice of $\{\sigma_i\}_{i=1}^n$; it is purely a linear algebra result. This observation gives us the following corollary.

Corollary 5. Let $\sigma_1, \ldots, \sigma_n \in \mathrm{Aut}(E)$, $\sigma_1 = \mathrm{id}_E$. Let $F \subset E$ be the fixed field of $\sigma_1, \ldots, \sigma_n$. Then we have $(E : F) \geq n$.

1.8. **(Optional) Constructions with straight-edge and compass.** We diverge from the notes to discuss a little on straight-edge and compass constructions, following Milne [4]. The idea follows from the Greeks; upon realizing that irrational numbers exist, they decided to expand $\mathbb{Q}$ to a set of numbers called the constructible numbers.

Definition. A real number is constructible if it can be "constructed" by forming successive intersections of

(1) lines drawn through two points already constructed, and
(2) circles with center a point already constructed and radius a constructed length.

We rewrite these rules in more algebraic terms. Throughout, F is a subfield of $\mathbb{R}$.

Definition. An F-line is a line in $\mathbb{R} \times \mathbb{R}$ through two points in the F-plane. That is, these are the lines given by equations

$$ax + by + c = 0, \quad a, b, c \in F.$$

Definition. An F-circle is a circle in $\mathbb{R} \times \mathbb{R}$ with center an F-point and radius an element of F. That is, these are the circles given by the equations

$$(x - a)^2 + (y - b)^2 = c^2, \quad a, b, c, \in F.$$

The idea, then, is to start with $F_0 = \mathbb{Q}$, and append all the points which lie along a F_0-line and a F_0-circle, and then call this new field F_1. We then append to F_1 the collection of all points which lie along an F_1-line and a F_1-circle. Continue this process ad-infinitum.

One immediate issue to this process is whether adjoining all these points still gives us a field. That is, is F_1 still a field so that we can try iterating the process again? The answer, it turns out, is yes.

Lemma 5 (**Lemma 1.35** [4])**.** (a) If c and d are constructible, then so are $c + d$, $-c$, cd, and c/d for $d \neq 0$.
(b) If $c > 0$ constructible, then so also is $\sqrt{c}$.

Proof. The idea is to first show that we can construct a line perpendicular to a given line through a given point. Thus, we are given a line $L : ax + by + c = 0$ and we wish to construct a perpendicular line. Relabeling this in a more familiar package, we have that the line is given by $L : y = mx + d$ so long as $b \neq 0$, and if $b = 0$ we have that it is given by $L : x = f$ for appropriate constants m, d, f. Given some point (x_0, y_0), we wish to find a perpendicular line through $L : y = mx + d$. Notice that we set $r = -m$, and solve $d = y_0 + rx_0$ to get a perpendicular line. Similarly, a perpendicular line for $L : x = f$ through the point (f, y_0) will be given by $L' : y = f$. Thus, we can find a perpendicular line through a given point (which will remain an F-line).

Next, we wish to show that we can construct a line through a chosen point (x_0, y_0) parallel to $L : y = mx + d$ (the other case is the same). Since the line is parallel, it has the same slope, and so we simply solve $y_0 = mx_0 + d$, and this gives us our parallel line through a point.

Thus, we have that we can construct triangles. Furthermore, given some triangle, we can construct a similar triangle using these processes. Appropriate choices of triangles gives us cd and c^{-1} are constructible. It follows easily that we have $c + d$, cd^{-1}, and $-c$ are constructible, and so we get (a).

For (b), construct a clever circle. That is, draw a circle of radius $(c+1)/2$ and center $(c+1)/2$, and draw a vertical line through the point $A = (1, 0)$ to meet the circle at P. The length AP will be $\sqrt{c}$. □

Thus, iterating this process does gives us a field F_n. That is, we have the following:

Corollary 6. $F = \bigcup_n F_n$ is a field.

The question, then, is how far do we get iterating this process. Geometrically, the three major questions for constructible numbers are the following:

(1) Is it possible to duplicate the cube using only lines and circles?
(2) Is it possible to trisect an angle using only lines and circles?
(3) Is it possible to square the circle by straight-edge and compass constructions?

The answer to all of these is no, as we will eventually see.

Lemma 6 (**Lemma 1.34** [4])**.** Let $L \neq L'$ be F-lines, and let $C \neq C'$ be F-circles.

(a) $L \cap L' = \varnothing$ or consists of a single F-point.
(b) $L \cap C = \varnothing$ or consists of one or two points in the $F[\sqrt{e}]$-plane for some $e \in F$ with $e > 0$.
(c) $C \cap C' = \varnothing$ or consists of one or two points in the $F[\sqrt{e}]$-plane for some $e \in F$ with $e > 0$.

Proof. The proof is just solving the simultaneous equations, which will be at most a quadratic equation with coefficients in F. □

It seems thus far that this has nothing to do with Galois theory. The following theorem connects to the two concepts.

Theorem 9 (**Theorem 1.36** [4])**.** A number α is constructible if and only if it is contained in a subfield of $\mathbb{R}$ of the form

$$\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_r}],$$

where the $a_i \in \mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}]$, $a_i > 0$.

Proof. The prior lemma tells us that every constructible number is contained in such a field. On the other hand, if all the elements of $\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}]$ are constructible, then $\sqrt{a_i}$ is constructible by **Lemma 5 (b)**. Applying **Lemma 5 (a)** gives $\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_i}]$ consists of constructible numbers. Thus, we have the desired result. □

Corollary 7. If α is constructible, then α is algebraic over $\mathbb{Q}$, and $(\mathbb{Q}[\alpha] : \mathbb{Q})$ is a power of 2.

Proof. By the prior theorem, a number α is constructible iff it is contained in some $\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_r}]$. Let's proceed by induction. Assume $z \in \mathbb{Q}[\sqrt{a}]$, where $a \in \mathbb{Q}$. Notice that $p(x) = x^2 - a \in \mathbb{Q}[x]$, and $\sqrt{a}$ is a root of this polynomial. Thus, $\sqrt{a}$ is algebraic. If $\sqrt{a} \in \mathbb{Q}$, then we see that p splits to $p(x) = (x - \sqrt{a})(x + \sqrt{a})$, the degree of the polynomial $x - \sqrt{a}$ will be 1, and so by prior we have that $\mathbb{Q}[\sqrt{a}] \cong F[x]/(x - \sqrt{a}) \cong \mathbb{Q}(\sqrt{a})$, so the field extension has degree

$$(\mathbb{Q}(\sqrt{a}) : \mathbb{Q}) = 1 = 2^0.$$

If $\sqrt{a} \notin \mathbb{Q}$, we get that $p(x)$ is the minimal polynomial, so by the same reasoning we have that

$$(\mathbb{Q}(\sqrt{a}) : \mathbb{Q}) = 2.$$

Assume now that $(\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{r-1}}) : \mathbb{Q}) = 2^j$ for some j. We wish to show that $a_r \in \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{r-1}})$ is such that $(\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{r-1}}, \sqrt{a_r}) : \mathbb{Q}) = 2^k$, where k is either $j + 1$ or j. By **Theorem 1**, we see that

$$\begin{aligned}(\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{r-1}}, \sqrt{a_r}) : \mathbb{Q}) &= (\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{r-1}}, \sqrt{a_r}) : \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{r-1}}))(\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{r-1}}) : \mathbb{Q}) \\ &= (\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{r-1}}, \sqrt{a_r}) : \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{r-1}}))2^j.\end{aligned}$$

If $\sqrt{a_r} \in \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{r-1}})$, we get that $x - \sqrt{a_r}$ is the minimal polynomial, so

$$(\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{r-1}}, \sqrt{a_r}) : \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{r-1}})) = 1$$

and hence

$$(\mathbb{Q}(\sqrt{a_1},\dots,\sqrt{a_{r-1}},\sqrt{a_r}):\mathbb{Q}) = 2^j.$$

If $\sqrt{a_r} \notin \mathbb{Q}(\sqrt{a_1},\dots,\sqrt{a_{r-1}})$, then the minimal polynomial is given by $x^2 - a_r$, so we get that

$$(\mathbb{Q}(\sqrt{a_1},\dots,\sqrt{a_{r-1}},\sqrt{a_r}):\mathbb{Q}(\sqrt{a_1},\dots,\sqrt{a_{r-1}})) = 2,$$

so

$$(\mathbb{Q}(\sqrt{a_1},\dots,\sqrt{a_{r-1}},\sqrt{a_r}):\mathbb{Q}) = 2^{j+1}.$$

□

Using this, we can answer some of our questions.

Corollary 8 (**Corollary 1.38** [4])**.** It is impossible to duplicate the cube by straight-edge and compass constructions.

Proof. It suffices to consider the unit cube. The goal, then, is to construct a cube with volume 2; thus, "doubling" the cube. This requires constructing the real root of the polynomial $x^3 - 2$. Using Eisenstein, this is irreducible, so we have $(\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}) = 3$; thus, it cannot be constructible. □

Corollary 9 (**Corollary 1.39** [4])**.** It is impossible to trisect an angle by a straight-edge and compass construction in general.

Proof. Consider an angle α. We wish to trisect 3α, which using some trig identities is the same as finding a solution to

$$\cos(3\alpha) = 4\cos^3(\alpha) - 3\cos(\alpha).$$

Taking α so that $\cos(\alpha) = 1/2$, we see that we have to solve $8x^3 - 6x - 1 = 0$. This is irreducible, since if there were a root $r = c/d$, $c \mid 1$, $d \mid 8$, and going through the options we see that none of these are roots. Consequently, $(\mathbb{Q}(\alpha):\mathbb{Q}) = 3$. □

Corollary 10 (**Corollary 1.40** [4])**.** It is impossible to square the circle by straight edge and compass constructions.

Proof. This is similar to the cube. Consider the circle with radius r. To square the circle, we need to find x so that $x^2 = \pi r^2$. Taking square roots, we see that x must be such that $x = \sqrt{\pi}r$. We have π is transcendental, so $\sqrt{\pi}$ must also be transcendental; consequently, x cannot be constructible. □

1.9. **(Optional) Tricks For Irreducibility.** In the last section, we used some tricks to determine irreducibility of polynomials. We formally introduce those here.

Proposition 1 (**Proposition 1.11** [4])**.** Let $r \in \mathbb{Q}$ be a root of the polynomial

$$a_m x^m + \cdots + a_0, \quad a_i \in \mathbb{Z}.$$

Write $r = c/d$, with $c, d \in \mathbb{Z}$ in reduced form. Then $c \mid a_0$, $d \mid a_m$.

Proof. Notice that

$$a_m \frac{c^m}{d^m} + \cdots + a_0 = 0.$$

Multiplying throughout by d^m, we have

$$a_m c^m + a_{m-1}c^{m-1}d + \cdots + a_0 d^m = 0.$$

Rearranging, we have

$$a_m c^m = d(-a_{m-1}c^{m-1} - \cdots - a_0 d^{m-1}).$$

Hence, $d \mid c^m a_m$. Since $(c, d) = 1$ (since they are in reduced form), we see that $d \nmid c^m$. Thus, $d \mid a_m$. A symmetric argument gives that $c \mid a_0$. □

Proposition 2 (Eisensteins Criterion, **Proposition 1.16** [4])**.** Let

$$p(x) = a_m x^m + \cdots + a_0, \quad a_i \in \mathbb{Z}.$$

That is, $p(x) \in \mathbb{Z}[x]$. Suppose there is a prime p such that

- p does not divide a_m,
- p divides $a_{m-1}, \ldots, a_0$,
- p^2 does not divide a_0.

Then p is irreducible in $\mathbb{Z}[x]$.

Proposition 3 (Gauss' Lemma, **Proposition 1.13** [4])**.** Let $p(x) \in \mathbb{Z}[x]$. If $p(x)$ factors non-trivially in $\mathbb{Q}[x]$, then it factors non-trivially in $\mathbb{Z}[x]$.

Instead of proving it, we make the useful observation.

Corollary 11. If $p(x)$ is irreducible in $\mathbb{Z}[x]$, then it is irreducible in $\mathbb{Q}[x]$.

Notice that this let's us extend the power of Eisenstein and the first proposition to $\mathbb{Q}[x]$. Furthermore, the arguments (see [4]) generalize to replacing $\mathbb{Z}$ with a UFD and $\mathbb{Q}$ with its field of fractions.

2. Galois Theory (Finite)

2.1. **Galois Extensions.** We now look at things from the point of view of the underlying field. Let $F \subset E$ be a subfield of E. Let $\sigma \in \mathrm{Aut}(E)$ be an automorphism of E.

Definition. We say that σ leaves F fixed if $\sigma|_F = \mathrm{id}$; in other words, $\sigma(x) = x$ for all $x \in F$.

Lemma 7. Consider the extension of fields E/F. The automorphisms that leave F fixed form a subgroup of $\mathrm{Aut}(E)$.

Proof. Since $\mathrm{Aut}(E)$ is a group, it suffices to show that $H = \{\sigma \in \mathrm{Aut}(E) : \sigma|_F = \mathrm{id}\}$ is a subgroup of $\mathrm{Aut}(E)$. Notice that the identity is in H, and if $\sigma, \tau \in H$, then we have

$$\sigma\tau^{-1}(x) = \sigma(\tau^{-1}(x)) = \sigma(x) = x,$$

so $\sigma\tau^{-1} \in H$. Hence, it's a subgroup (so a group on its own right). □

We denote the collection of automorphisms of E that leave F fixed as $\mathrm{Gal}(E/F)$.

Remark. Notice that we have the concept of fixed fields and fields fixed by automorphisms. Note that these are different; that is, the field fixed by $\mathrm{Gal}(E/F)$ does not necessarily have to be F, but F will be contained in it.

Throughout, we will let $G = \mathrm{Gal}(E/F)$. Let

$$E^G = \{\alpha \in E : \sigma(\alpha) = \alpha \forall \alpha \in G\}.$$

As observed above, we have $F \subset E^G$.

Definition. A (finite) extension E/F is called Galois if the following hold:
(1) $(E : F) < \infty$,
(2) If $G = \mathrm{Gal}(E/F)$, then $F = E^G$.

Note that Artin calls such extensions normal. Normal in todays context has a different meaning.

Definition. An extension E/F is called normal if it is algebraic and every irreducible $p(x) \in F[x]$ which has a root $\alpha \in E$ splits completely in E, i.e., E contains a splitting field of the minimal polynomial $f_\alpha(x) \in F[x]$ for every $\alpha \in E$.

For Galois extensions we have the following result for the degree of the extension.

Theorem 10. Let E be a field, $G = \{\sigma_1, \ldots, \sigma_n\} \leq \mathrm{Aut}(E)$ a subgroup. If $F = E^G$, then $(E : F) = n$.

Proof. Note that G is a group, hence, without loss of generality, we have that $\sigma_1 = \mathrm{id}$. Thus, we have

$$F = E^G = \{\alpha \in E : \sigma_i(\alpha) = \alpha \forall \sigma_i \in G\}$$

is such that $(E : F) \geq n$. It suffices to show that $(E : F) \leq n$. Assume for contradiction that $(E : F) > n$. The goal is to do the same trick as last time. Since $(E : F) > n$, there exists $\alpha_1, \ldots, \alpha_{n+1} \in E$ that are linearly independent over F. Thus, we can set up a system

$$\sum_1^{n+1} \sigma_j(\alpha_i) x_i = 0, \quad j = 1, \ldots, n.$$

There are more unknowns than equations, so there exists a non-trivial solution $\beta_1, \ldots, \beta_{n+1}$. If the $\beta_i \in F$, we would have that

$$\sum_1^{n+1} \alpha_i \beta_i = 0$$

is a non-trivial relation (here, using $\sigma_1 = \mathrm{id}$), contradicting the fact that the α_i are linearly independent over F. Thus, the $\beta_i \notin F$.

Among all of the non-trivial solutions, we will choose the one which has the least number of non-zero entries. Reorder so that we have tha the solution is going to be $\beta_1, \ldots, \beta_r$, $\beta_i \neq 0$ for $i = 1, \ldots, r$. Notice that $r > 1$, since otherwise we have

$$\beta_1 \sigma_1(\alpha_1) = 0 \implies \beta_1 = 0.$$

Divide all of the entries by β_r; label $\widetilde{\beta}_i = \beta_i / \beta_r$ for $1 \leq i \leq r - 1$. The system then becomes

$$\sum_1^{r-1} \sigma_j(\alpha_i) \widetilde{\beta}_i + \sigma_j(\alpha_r) = 0, \quad j = 1, \ldots, n.$$

By what we've noticed earlier, we must have that there exists a $\widetilde{\beta}_i \in E/F$. Without loss of generality, let's set it to be $\widetilde{\beta}_1$. Then we have a σ_k so that

$$\sigma_k(\widetilde{\beta}_1) \neq \widetilde{\beta}_1.$$

Now, apply σ_k to our system; we get the system

$$\sum_1^{r-1} \sigma_k(\sigma_j(\alpha_i)) \sigma_k(\widetilde{\beta}_i) + \sigma_k(\sigma_j(\alpha_r)) = 0, \quad j = 1, \ldots, n.$$

G is a group, so notice that $\sigma_k \cdot \{\sigma_1, \ldots, \sigma_n\} = \{\sigma_1, \ldots, \sigma_n\}$. Up to relabeling, then, we have the system

$$\sum_1^{r-1} \sigma_j(\alpha_i) \sigma_k(\widetilde{\beta}_i) + \sigma_j(\alpha_r) = 0.$$

Substracting this system from the first, we get

$$\sum_1^{r-1} \sigma_j(\alpha_i) \left[\widetilde{\beta}_i - \sigma_k(\widetilde{\beta}_i) \right] = 0.$$

Hence, we have that $\widetilde{\beta_1} - \sigma_k(\widetilde{\beta_1}, \ldots, \widetilde{\beta_{r-1}} - \sigma_k(\widetilde{\beta_{r-1}})$ is another solution of our system. By the choice of σ_k, we have

$$\widetilde{\beta_1} - \sigma_k(\widetilde{\beta_1}) \neq 0.$$

This is our contradiction; we have a set which is non-trivial, and which has less non-zero elements, contradicting the minimality of the solution $\beta_1, \ldots, \beta_{r-1}$. This gives $(E : F) \leq n$, and so $(E : F) = n$. □

Corollary 12. If $G \subset \mathrm{Aut}(E)$ is a finite group and $F = E^G$, then $G = \mathrm{Gal}(E/F)$.

Proof. We have that $(E : F) = n = |G|$. Suppose that there was a $\sigma \in \mathrm{Aut}(E)$ such that $\sigma \notin G$ but $\sigma(a) = a$ for all $x \in F$. Then F is fixed by $n + 1$ distinct elements of $\mathrm{Aut}(E)$. Notice that **Corollary 5** tells us that $(E : F) \geq n + 1$, which is a contradiction. □

Corollary 13. Let G_1, G_2 be finite subgroups of $\mathrm{Aut}(E)$ with $G_1 \neq G_2$. Then

$$E^{G_1} = F_1 \neq F_2 = E^{G_2}.$$

Proof. If $F_1 = F_2 = F$, then

$$G_1 = \{\sigma \in \mathrm{Aut}(E) : \sigma(a) = a \text{ for all } a \in F\} = G_2.$$

□

2.2. **Separable Extensions.** The idea of separable extensions of fields is to connect automorphisms of fields to properties of polynomials.

Definition. (i) Let $p(x) \in F[x]$. We call $p(x)$ separable if its *irreducible factors* do not have repeated roots in a splitting field.

(ii) If E/F is an extension, an element $\alpha \in E$ is called separable over F if it is the root of a separable polynomial $p(x) \in F[x]$. That is, its minimal polynomial $p_\alpha(x)$ is separable.

(iii) The extension E/F is called separable if every $\alpha \in E$ is separable over F.

Example. A non-intuitive example might be examining $p(x) = (x - 3)^2 \in \mathbb{Q}[x]$. The gut feeling from the definition would be that this is not separable; however, notice that each of the irreducible factors must not have repeated roots. The irreducible factors here are $(x - 3)$, so there are no repeated roots to worry about.

Example (**Exercise 2.59** [6])**.** We will prove that, for characteristic 0 fields, we have that every irreducible polynomial is separable (hence, every polynomial is separable, per our definition). Let F be a field. Consider the operator

$$D : F[x] \to F[x],$$

where if

$$p(x) = \sum_{i=0}^{n} a_i x^i,$$

then

$$D(p(x)) = \sum_{i=1}^{n} i a_i x^{i-1}.$$

In other words, this is the formal derivative of a polynomial. Essentially, D is defined via setting

$$D(x) = 1,$$

and

$$D(p(x)q(x)) = D(p(x))q(x) + p(x)D(q(x)),$$

i.e. its established by the product rule and the power rule, and then linearly extending this operation. Consequently, D is a linear operator.

We first show the following lemma.

Lemma 8. $p(x) \in F[x]$ is separable if and only if $\gcd(p(x), D(p(x))) = 1$ (1 here is the multiplicative identity in F).

Proof. Assume first $p(x)$ is separable. Let α be a root of $p(x)$. Then we have that $(\alpha - x)h(x) = p(x)$ for some $h(x)$ with $h(\alpha) \neq 0$ (this holds since the polynomial is separable; we have no repeated roots). Taking the formal derivative and applying the product rule, we get

$$(\alpha - x)D(h(x)) - h(x) = D(p(x)).$$

Plugging in $x = \alpha$, we have

$$-h(\alpha) = D(p(\alpha)) \neq 0,$$

so α is not a root of $D(p(x))$. This holds for all roots of $p(x)$, so $p(x)$ and $D(p(x))$ do not share a root; notice this forces their gcd to be 1.

Assume $p(x)$ is not separable. Let α be a repeated root. Thus, we have $p(x) = (\alpha - x)^2 h(x)$, where $h(\alpha)$ may or may not be zero (it will not matter). Applying the product rule here gives us

$$D(p(x)) = 2(\alpha - x)h(x) + D(h(x))(\alpha - x)^2,$$

which we see will be zero at $x = \alpha$. Thus, they share a root, and so their gcd is not 1. □

We can now deduce the following.

Corollary 14. For fields of characteristic 0, every polynomial is separable.

Proof. Without loss of generality, it suffices to consider irreducible polynomials (per the definition). By the lemma, it suffices to show that if $p(x)$ is irreducible, then $\gcd(p(x), D(p(x))) = 1$. Assume otherwise; that is, $\gcd(p(x), D(p(x))) = h(x) \neq 1$. Since $p(t)$ is irreducible, this implies that $h(x) = rp(x)$ for some element r, and we have $rp(x) \mid D(p(x))$; that is, $p(x) \mid D(p(x))$. Notice that $\deg(D(p(x))) < \deg(p(x))$, so the only way this can happen is if $D(p(x)) = 0$. In a characteristic 0 field, the only way that the derivative can be 0 is if the polynomial was constant; this tells us that irreducible polynomials are separable, since by definition they are non-constant. Hence, all irreducible factors of a polynomial will be separable, so every polynomial is separable in a characteristic 0 field. □

We also get for free a classification of irreducible non-separable polynomials in fields of characteristic p.

Corollary 15. Let F be a field of characteristic $p \neq 0$. If $p(x) \in F[x]$ is irreducible and not separable, then it is of the form $q(x^p) = p(x)$ for some $q(x) \in F[x]$.

Proof. Assuming $p(x) \in F[x]$ is irreducible and not-separable, we have that the lemma tells us $\gcd(p(x), D(p(x))) \neq 1$. From our observation in the prior corollary, we see that this tells us that $D(p(x)) = 0$. Notice that, for the polynomial $p(x)$ to be non-constant, we need

$$D(p(x)) = \sum_{i=1}^{n} i a_i x^{i-1} = 0.$$

This implies $p \mid ia_i$ for $1 \leq i \leq n$. Since p is prime, we have that this implies $p \mid i$ or $p \mid a_i$. If $p \mid a_i$, this tells us that the coefficient was 0 all along, and so there was nothing to differentiate. Thus, we must have $p \mid i$, so that $p(x)$ is of the form

$$p(x) = \sum_{i=1}^{n} a_i x^{k_i p} = \sum_{i=1}^{n} a_i (x^p)^{k_i},$$

where the k_i are some integers. Thus, setting

$$q(x) = \sum_{i=1}^{n} a_i x^{k_i},$$

we have $p(x) = q(x^p)$. □

Notice the relation here with the Frobenius endomorphism.

We now get the relation between automorphisms of E and the splitting of polynomials in the following theorem.

Theorem 11. We have that E/F is a finite Galois extension if and only if E is the splitting field of a separable polynomial $p(x) \in F[x]$.

Proof. ($\implies$): We start with a lemma.

Lemma 9. If E/F is a finite Galois extension, then E/F is separable and normal.

Proof. By assumption, we have $(E : F) < \infty$ and $G = \mathrm{Gal}(E/F)$ is such that $F = E^G$. There are two things we wish to show:

(1) E/F is algebraic and every irreducible $p(x) \in F[x]$ which has a root $\alpha \in E$ splits completely (normal).
(2) For all $\alpha \in E$, there exists a separable polynomial $p(x) \in F[x]$ so that $p(\alpha) = 0$ (separable).

We do both simultaneously. Write out $G = \{\sigma_1, \ldots, \sigma_n\}$ with $\sigma_1 = \mathrm{id}$. Let $\alpha \in E$. Let $\{\alpha_1, \ldots, \alpha_n\}$ be the orbit of α under G, i.e. $\alpha_i = \sigma_i(\alpha)$ (note that we may have repeats here). Eliminating repeats, we are left with the set $\{\alpha_1, \ldots, \alpha_r\}$. Since G is a group, the α_i are permuted among each other by G. Therefore, the polynomial

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_r)$$

is fixed by G. Notice that this means that

$$\sigma_i(f(x)) = \sigma_i(x - \alpha_1) \cdots \sigma_i(x - \alpha_r) = (x - \alpha_1) \cdots (x - \alpha_r) = f(x).$$

Writing out the coefficients of f, we see that this implies that the coefficients are fixed under the σ_i. Since $F = E^G$, this tells us that the coefficients are in F; that is, we have $f(x) \in F[x]$.

Let $g(x) \in F[x]$ be such that it has α as a root. Writing out g, we have

$$g(x) = \sum_{i=0}^{n} a_i x^i.$$

Applying σ_j to $g(\alpha)$, we have

$$0 = \sigma_j(g(\alpha)) = \sum_{i=0}^{n} a_i \sigma_j(\alpha)^i = \sum_{i=0}^{n} a_i \alpha_k^i = g(\alpha_k),$$

where $\alpha_k \in \{\alpha_1, \ldots, \alpha_r\}$. Thus, we have that g has the α_k as roots as well, so $f(x) \mid g(x)$. Notice this applies for any polynomial which has α as a root, so $f(x)$ must be the minimal polynomial for α. This also forces f to be irreducible. Since the minimal polynomial for every α is separable and splits completely, this tells us that E/F satisfies (1) and (2). Thus, E/F is separable and normal. □

Going back to the theorem, suppose E/F is a finite Galois extension. Let $\omega_1, \ldots, \omega_t$ be a basis of E/F. Let $f_i(x) \in F[x]$ be the separable irreducible polynomial having ω_i as a root. Taking $f(x) = f_1(x) \cdots f_t(x) \in F[x]$, we see that this is separable (since each irreducible component is separable) and E is the splitting field of f since each f_i splits completely by normality. Thus, we

have the forward direction.
($\Longleftarrow$): Let E be the splitting field of a separable polynomial $p(x) \in F[x]$. The goal is to construct the Galois group. First observe that if all of the roots of $p(x)$ are in F, then we are done by setting $E = F$ and $G = \{\text{id}\}$.

We induct now on the number of roots of $p(x)$ which do *not* lie in F. Let n denote this number. Suppose that $p(x)$ has $n > 1$ roots in $E \setminus F$, but for all pairs of field $K \subset E$ with fewer than n roots of $p(x)$ outside of K, the proposition holds. That is, for all fields $F \subset K \subset E$ where $p(x)$ has fewer than n roots outside of K, we get that K/E is a finite Galois extension. Write $p(x) = p_1(x) \cdots p_r(x)$ as the factorization of $p(x)$ into irreducible factors in $F[x]$. Notice that one of them must have degree greater than 1, since otherwise all of the roots belong to F, reducing us to our trivial case. Without loss of generality, let's take this to be the first factor; suppose $\deg(p_1) = s > 1$. If α_1 is a root of $p_1(x)$, then $F \subset F(\alpha_1) \subset F$, and $(F(\alpha_1) : F) = s = \deg(p_1)$ (by **Corollary 2**).

Now, $E/F(\alpha_1)$ is still the splitting field of $p(x) = 0$, and the number of roots of $p(x)$ outside of $F(\alpha_1)$ is going to be less than n, since $\alpha_1 \in F(\alpha_1)$. Therefore, the theorem holds for $F(\alpha_1)$, and so we have $E/F(\alpha_1)$ is a finite Galois extension. Let $G_1 = \text{Gal}(E/F(\alpha_1))$. Since $p9x)$ was separable, the roots $\alpha_1, \ldots, \alpha_s$ of $p_1(x)$ are distinct in E. For each root α_i, there exists a σ_i so that $\sigma_i(\alpha_1) = \alpha_i$. Thus, $\sigma_i : F(\alpha_1) \to F(\alpha_i)$ is a field isomorphism leaving F invariant. We can extend the σ_i uniquely to an element of $\text{Aut}(E)$, which we'll also denote by σ_i. This gives us a collection $\{\sigma_1, \ldots, \sigma_s\} \subset \text{Aut}(E)$ which leaves F fixed.

Let $G = \text{Gal}(E/F) = \{\sigma \in \text{Aut}(E) : \sigma(a) = a \text{ for all } a \in F\}$. Suppose $\theta \in E^G$, the fixed field of G. The goal is to show $\theta \in F$, giving us $E^G = F$. Notice that $\text{Gal}(E/F(\alpha_1)) = G_1 \subset G = \text{Gal}(E/F)$. Due to this, we have the relation that $E^G \subset F(\alpha_1)$; that is, if θ is fixed by all of the $\sigma \in G$, then it is in particular fixed by all the $\sigma \in G_1$, and since it's a Galois extension we see that $\theta \in E^{G_1} = F(\alpha_1)$.

Since $\theta \in F(\alpha_1)$, we have that

$$\theta = \sum_{i=0}^{s-1} c_i \alpha_1^i, \quad c_i \in F.$$

Applying $\sigma_i \in G$, we have

$$\sigma_i(\theta) = \theta = c_0 + c_1\alpha_i + \cdots + c_{s-1}\alpha_i^{s-1} \in F(\alpha_i).$$

We claim now that the polynomial

$$g(x) = (c_0 - \theta) + c_1 x + \cdots + c_{s-1}x^{s-1} \in F[x]$$

has $\alpha_1, \ldots, \alpha_s$ for roots. To see this, notice that

$$\begin{aligned} g(\alpha_i) &= (c_0 - \theta) + c_1\alpha_i + \cdots + c_{s-1}\alpha_i^{s-1} \\ &= \left(c_0 - \left[c_0 + c_1\alpha_i + \cdots + c_{s-1}\alpha_i^{s-1}\right]\right) + c_1\alpha_i + \cdots + c_{s-1}\alpha_i^{s-1} = 0. \end{aligned}$$

Notice this is more roots than the degree of the polynomial, which is impossible unless $g(x) = 0$. So we get $g(x) = c_0 - \theta = 0$; that is, $c_0 = \theta$. So $\theta \in F$. The choice of θ was arbitrary, and thus we get $E^G \subset F$; apriori, we have $F \subset E^G$, so $E^G = F$. Thus, E/F is Galois, since the degree of the extension was finite by assumption. □

Definition. If E/F is the splitting field of a separable polynomial $f(x) \in F[x]$, we will call $\text{Gal}(E/F) = G_f$ the Galois group of the polynomial $f(x)$.

Remark. Note that we can extend **Theorem 11** to the following.

Theorem 12 (**Theorem 3.10** [4])**.** For an extension E/F, the following are equivalent:
(a) E is the splitting field of a separable polynomial $f \in F[x]$.
(b) E/F is a finite Galois extension.

(c) $F = E^G$ for some finite group G of automorphisms of E.
(d) E is normal, separable, and finite over F.

Proof. We showed in **Theorem 11** $(a) \iff (b)$. Notice **Lemma 9** establishes $(b) \implies (d)$, and we have $(b) \iff (c)$ by definition. We only need to show $(d) \implies (a)$.
$(d) \implies (a)$: Since $(E : F) < \infty$, it is generated over F by a finite number of elements, say $E = F[\alpha_1, \ldots, \alpha_m]$, where $\alpha_i \in E$. Taking f_i to be the minimum polynomial over the α_i, and f to be the product of the f_i, we get that each f_i splits in E by normality, so E is the splitting field of f. Notice f is separable, since E is separable over F, so each of the f_i are separable. □

Thus, we have three different ways of defining a finite Galois extension.

2.3. **Fundamental Theorem of Finite Galois Theory.** We are now at the fundamental theorem for finite Galois theory.

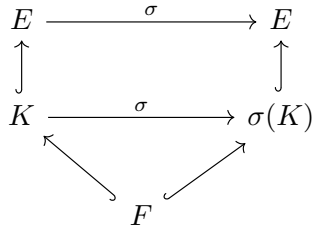
Theorem 13 (Fundamental Theorem for Finite Galois Theory)**.** Let $p(x) \in F[x]$ be separable, E/F the splitting field of $p(x)$, and $G = \mathrm{Gal}(E/F) = G_p$. Then we have the following:

(1) Every intermediate field $F \subset K \subset E$ is the fixed field $E^H = K$ for some subgroup $H < G$. Distinct subgroups have distinct splitting fields, so
$$K = E^H \text{ and } H = \mathrm{Gal}(E/K).$$
(2) K/F is Galois if and only if $H \trianglelefteq G$. That is, K/F is Galois if and only if $E^H = K$ and H is a normal subgroup of G. In this case, we get
$$\mathrm{Gal}(K/F) \cong G/H.$$
(3) If $F \subset K \subset E$ and $H = \mathrm{Gal}(E/K)$, then $(K : F) = (G : H)$ and $(E : K) = |H|$.

Proof. (1) If $F \subset K \subset E$, then E is still the splitting field of $p(x) \in F[x] \subset K[x]$ over K, $p(x)$ a separable polynomial by **Theorem 12**. Thus, invoking **Theorem 12** again, we get that E/K is Galois. If $H = \mathrm{Gal}(E/K)$, then we note that $H < G$ and $K = E^H$. To see that $H < G$, we have that if $\sigma \in H$, then σ fixes K, and $F \subset K$, so σ also fixes F, and hence $\sigma \in G$. To see that $E^H = K$, we use **Theorem 12**.

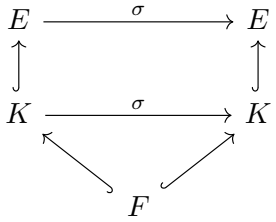
Remark. An aside now is that we've seen that distinct subgroups of G have distinct fixed fields (**Corollary 13**). So there is an order reversing bijection between intermediate fields and subgroups of the Galois group.

(2) Now consider an intermediate field $F \subset K \subset E$ and $H = \mathrm{Gal}(E/K)$. If $\sigma \in \mathrm{Gal}(E/F) = G$, then $\sigma(E) = E$ and $\sigma(K) \subset \sigma(E) = E$ is another intermediate field (possibly still K). Thus, we have the following:



If $\tau \in H = \mathrm{Gal}(E/K)$, then $\tau(K) = K$ and $\sigma\tau(K) = \sigma(K)$. So elements in the same coset in G/H give the same conjugate intermediate field. Next, if σ_1, σ_2 lie in distinct cosets of G/H, then σ_1 and σ_2 give distinct isomorphisms of intermediate fields $\sigma_1(K)$ and $\sigma_2(K)$. This is due to the fact if $\sigma_1(a) = \sigma_2(a)$ for all a, then $\sigma_2^{-1}\sigma_1(a) = a$ for all $a \in K$, and so $\sigma_2^{-1}\sigma_1 \in H$. That is, $\sigma_1 \in \sigma_2 H$.

The next thing to note is that if K_1 and K_2 are two intermediate fields and $\sigma : K_1 \to K_2$ over F, then since E is still the splitting field of $p(x)$ over K_1 and K_2, any isomorphism over F extends to an isomorphism of the splitting field E over F; i.e., this isomorphism σ is an element of $\mathrm{Gal}(E/F)$. So it gives us a diagram



Together, these give that the distinct embeddings $\sigma : K \hookrightarrow E$ all come from restricting $\sigma \in \mathrm{Gal}(E/F)$. The number of such embeddings then is going to be the number of cosets; i.e., $(G : H) = |G/H|$.

With these, we can start to prove (2). Suppose K/F is Galois. Then we know that $|\mathrm{Gal}(K/F)| = (K : F)$. For the converse, let $F' = K^{\mathrm{Gal}(K/F)}$. Then $F \subset F' \subset K$. But we have

$$(K : F') = |\mathrm{Gal}(K/F)|,$$

so we get that $F = F'$. Hence, K is Galois over F. Thus, K is Galois over F if and only if $(K : F) = |\mathrm{Gal}(K/F)|$. But

$$|\mathrm{Gal}(K/F)| = (K : F) = (G : H) = |G/H|,$$

or its equal to the number of distinct embeddings of K into E. Thus, the number of distinct embeddings is equal to the number of isomorphisms, and so we have that $\sigma(K) = K$ fo rall $\sigma \in \mathrm{Gal}(E/F)$. So

$$\begin{aligned} K/F \text{ is Galois} &\iff |\mathrm{Gal}(K/F)| = (K : F) \\ &\iff \sigma(K) = K \text{ for all } \sigma \in \mathrm{Gal}(E/F) \\ &\iff \sigma H \sigma^{-1} = H \text{ for all } \sigma \in \mathrm{Gal}(E/F) \\ &\iff H \trianglelefteq G. \end{aligned}$$

Note that the number of distinct embeddings is isomorphic to G/H, the number of distinct automorphisms of K fixing F is $\mathrm{Gal}(K/F)$, and so we get $\mathrm{Gal}(K/F) \cong G/H$.

(3) Given (1), we see that

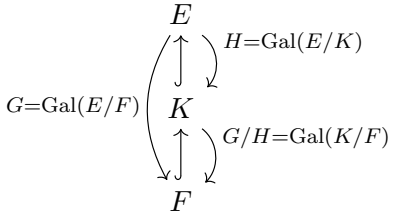
$$(E : K) = |\mathrm{Gal}(E/K)| = |H|$$

and

$$(K : F) = (E : F)/(E : K) = |G|/|H| = |G/H| = (G : H).$$

□

We remark that if $F \subset K \subset E$ with K/F Galois, then we have the field diagrams



3. Finite Fields

3.1. **Preliminaries.** We start with the following.

Theorem 14. Let F be a field, S a finite subgroup of $F^\times$. Then S is a cyclic group.

Proof. We use the structure theorem for finitely generated abelian groups, which says that if G is a finitely generated abelian group, then

$$G \cong C_1 \oplus \cdots \oplus C_t,$$

where each C_i is cyclic, $|C_i|$ divides $|C_{i+1}|$, and t is the minimum number of generators of G. One consequence of this is that if G is a finite abelian group and $m = |C_t|$, then every element of G has order dividing m. So since S is a finite abelian group, we have

$$S \cong C_1 \oplus \cdots \oplus C_t,$$

and the exponent of S is $m = |C_t|$. Thus, every element of S satisfies the following polynomial relation:

$$x^m - 1 = 0.$$

Let $n = |S|$. Since $x^m - 1$ can have at most m roots, $m \geq n$. Since the order of any element of S divides $|S| = n$, we have $m \mid n$, so $m \leq n$. Therefore, $m = n$. Since $C_t = \langle \alpha \rangle$ has order m, $S = \langle \alpha \rangle = C_t$. □

From this, we get a nice fact on finite fields.

Corollary 16. If F is a finite field, $F^\times$ is the set of units, then $F^\times$ is cyclic.

3.2. **The Characteristic of a Field.** Now, let F be an arbitrary field. We have a map

$$\phi : \mathbb{Z} \to F$$

where

$$\phi(n) = (1 + 1 + \cdots + 1)$$

n times. We consider the two cases here:

Case 1: If $\mathrm{Ker}(\phi) = 0$, then $\phi : \mathbb{Z} \to F$ and $\mathbb{Z} \subset F$. The field of fractions is the smallest field containing a ring, so we get that $\mathbb{Q} \subset F$ as well. In this case, the field has characteristic 0.

Case 2: If $\mathrm{Ker}(\phi) \neq 0$, then since $\mathrm{Im}(\phi) \subset F$ is a domain, $\mathrm{Ker}(\phi) = p\mathbb{Z}$ for some prime p. Thus,

$$\phi : \mathbb{Z}/p\mathbb{Z} \hookrightarrow F.$$

In this case, the field has characteristic $p > 0$.

We denote the characteristic of a field F by $\mathrm{Char}(F)$. Note that if $\mathrm{Char}(F) = p$, then for any $\alpha \in F$, we have that

$$p \cdot \alpha = (\alpha + \alpha + \cdots + \alpha) = \alpha(1 + 1 + \cdots + 1) = \alpha \cdot 0 = 0.$$

We can make a general statement on the characteristic of a finite field.

Theorem 15. If F is a finite field, then $\mathrm{Char}(F) = p$ for some prime p, and $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \subset F$.

Note here that $\mathbb{F}_p$ is the field with p elements.

Proof. Consider $\phi : \mathbb{Z} \to F$. We have that $\mathrm{Ker}(\phi) \neq 0$, since otherwise we have that $|F| = \infty$. Recall that the kernel of a ring homomorphism is a prime ideal, so we have that $\mathrm{Ker}(\phi) = p\mathbb{Z}$ for some prime p. Thus, we have that the characteristic is p for some prime p. □

Corollary 17. If F is a finite field, then $|F| = p^\nu = q$ for some $\nu \geq 1$.

Proof. F is a finite dimensional vector space over $\mathbb{F}_p$. If $(F : \mathbb{F}_p) = \nu$, then $|F| = |\mathbb{F}_p|^\nu = p^\nu$. □

Note that if F is a finite field, then it is canonically the splitting field of a polynomial.

Theorem 16. Let F be a finite field of characteristic p. Then $|F| = q = p^\nu$ for some $\nu \geq 1$. We have that F is the splitting field of

$$x^q - x$$

over $\mathbb{F}_p$.

Proof. Note that, since $F^\times$ is cyclic of order $q-1$, we get that

$$x^{q-1} - 1 = 0$$

for all $x \in F^\times$. Hence,

$$x^{q-1} - 1 = \prod_{a \in F^\times} (x - a).$$

Appending x, we get

$$x^q - x = x(x^{q-1} - 1) = \prod_{a \in F^\times} (x-a) \cdot (x - 0) = \prod_{a \in F} (x - a).$$

So if $\mathbb{F}_p \subset F$ is the prime field generated by 1, then F is the splitting field of $x^q - x$ over $\mathbb{F}_p$. □

Corollary 18. If $|F| = q = p^\nu$, then $F = \{a : a \text{ is a root of } x^q - x = 0\}$.

Corollary 19. Any two finite fields of the same order are isomorphic.

Proof. Let $|F| = |F'| = q$. Then if $\mathbb{F}_p$ and $\mathbb{F}'_p$ are their prime fields, then $\mathbb{F}_p \cong \mathbb{F}'_p$. F is the splitting field of $x^q - x$ over $\mathbb{F}_p$, F' is the splitting field of $x^q - x$ over $\mathbb{F}'_p$, and **Theorem 6** gives us that $F \cong F'$. □

3.3. **Separability and Differentiation.** We're back to letting F be any field again. If $f(x) = a_0 + \cdots + a_n x^n \in F[x]$, we can define its formal derivative as

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}.$$

Note that we have the following:

(1) $(p(x) + q(x))' = p'(x) + q'(x)$,
(2) $(p(x) \cdot q(x))' = p'(x)q(x) + p(x)q'(x)$,
(3) $(p^n(x))' = np^{n-1}(x)p'(x)$.

The formal derivative gives us a practical test for a polynomial to have repeated roots. For irreducible polynomials, then, we have a test for separability.

Theorem 17. Let $f(x) \in F[x]$. Then the following are equivalent:

(i) $f(x)$ has repeated roots.
(ii) In a splitting field E of f, $f(x)$ and $f'(x)$ have a common root.
(iii) $\gcd(f, f') > 1$ in $F[x]$.

Proof. We showed the equivalence of $(i) \iff (iii)$ in **Lemma 8**. It suffices to show $(i) \iff (ii)$, then. Let α be a root of $f(x) = 0$ in E. Suppose the multiplicity of α is k, so

$$f(x) = (x - a)^k q(x)$$

in $E[x]$, $q(a) \neq 0$. Using the product rule, we get

$$f'(x) = (x-a)^{k-1} \left[(x-a)q'(x) + kq(x) \right].$$

If $k \geq 1$, then α is a root of $f'(x)$ of multiplicity $k-1$. If $k = 1$, then it's not a root. So we have $(i) \iff (ii)$. □

Recall **Corollary 14** and **Corollary 15**, which told us that in $\mathrm{Char}(F) = 0$, we have that every polynomial is separable, and if $\mathrm{Char}(F) = p$ then things were afoot. This leads us to the definition of perfect fields.

Definition. A field F is perfect if every irreducible polynomial $f(x) \in F[x]$ is separable.

Note then that the Corollary we proved was that if $\mathrm{Char}(F) = 0$, then F is perfect. A more surprising result is the following.

Theorem 18. If F is a finite field, then F is perfect.

Proof. We show first the following.

Lemma 10. A field F is perfect if and only if it has characteristic 0 or it has characteristic p and $F^p = F$.

Proof. ($\implies$): Assume that the field F is perfect and $\mathrm{Char}(F) = p > 0$. Assume as well (for contradiction) that $F^p \neq F$. Since $F^p \neq F$, there exists a $r \in F \setminus F^p$. Examine the polynomial $p(x) = x^p - r \in F[x]$. In the splitting field for this polynomial, we see that it splits as $p(x) = (x-t)^p$, where t is such that $t^p = r$. We claim that the polynomial is irreducible in $F[x]$. Since it splits as $(x-t)^p$, we see that any monic non-trivial factor will be of the form $(x-t)^m$, $1 \leq m \leq p-1$. Expanding this with the binomial theorem, we have

$$(x-t)^m = \sum_{j=0}^{m} \binom{m}{j} x^j (-t)^{m-j}.$$

If this were in $F[x]$, we have that $\binom{m}{j}(-t)^{m-j} \in F$ for $0 \leq j \leq m$. Examining the $m-1$ coefficient, we get that this implies that $-mt^{m-1} \in F$ for $1 \leq m \leq p-1$. Since $m \neq 0$, we get that $m \in \mathbb{F}_p^\times \subset F^\times$, which then forces $t \in F$. This means that $r \in F^p$, which is a contradiction. Since the field is perfect, though, we must have that its separable, and thus we have the contradiction.
($\impliedby$): Assume that it is not perfect; in other words, $\mathrm{Char}(F) = p > 0$ and there is a separable irreducible polynomial, say $p(x) \in F[x]$. By what we've established, this happens if and only if $p'(x) = 0$, and so $p(x)$ is a polynomial of the form $p(x) = q(x^p)$, where $q(x) \in F[x]$. Writing it out explicitly, we have

$$p(x) = a_0 + a_1 x^p + \cdots + a_n x^{np}.$$

If $F^p = F$, we have that $a_i = b_i^p$ for some $b_i \in F$, so

$$p(x) = b_0^p + (b_1 x)^p + \cdots + (b_n x^n)^p.$$

Notice that

$$(b_0 + b_1 x + \cdots + b_n x^n)^p = b_0^p + (b_1 x)^p + \cdots + (b_n x^n)^p = p(x)$$

by the binomial theorem. This contradicts the fact that $f(x)$ is irreducible, so we cannot have $F^p = F$. Thus, we've shown that if $\mathrm{Char}(F) = 0$ or if $\mathrm{Char}(F) = p > 0$ and $F^p = F$, then the field is perfect. □

By this lemma, it suffices to show that if F is a finite field of characteristic p, then $F^p = F$. Notice that the map $\phi : F \to F$ given by $\phi(x) = x^p$ is injective (since if $\phi(x) = \phi(y)$, we have $x^p = y^p$, so $x = y$). Since F is finite, and we have an injective linear map between fields, we see that this forces ϕ to be an isomorphism, so $\phi(F) = F^p = F$. □

4. Connected Topics

4.1. **Cyclotomic Fields.** We obtain cyclotomic fields from a base field F by adjoining roots of unity. One reason to study cyclotomic fields is that they are good sources of abelian extensions, where we define abelian extensions as extensions with abelian Galois group. A theorem of Kronecker and Weber says that if the base field is $\mathbb{Q}$, then every abelian extension of $\mathbb{Q}$ is a subfield of a cyclotomic field.

Let F be any field and consider the polynomial

$$p(x) = x^n - 1 \in F[x].$$

If n is not divisible by the characteristic of the field, then $x^n - 1$ has no repeated roots, since nx^{n-1} is not 0 (since n is not divisible by p, and this only has $x = 0$ as a root. So we get $\gcd((x^n - 1), D(x^n - 1)) = 1$ and $x^n - 1$ is separable over F. From here on, we will assume $\gcd(n, p) = 1$.

Let E/F be the splitting field of $x^n - 1$. We will call E the nth cyclotomic field over F. Since $x^n - 1$ is separable, E/F is a Galois extension. The set of roots of $x^n - 1$, denoted by S, forms a finite multiplicative subgroup of $E^\times$. To see this, note that $1 \in S$, and let $a, b \in S$. The goal is to show that $ab \in S$. Notice that we have

$$a^n = 1, \quad b^n = 1, \quad (ab)^n - 1 = a^n b^n - 1 = 1 - 1 = 0,$$

so $ab \in S$. Thus, it is cyclic by **Theorem 14**. Let ζ_n be any generator of this group. We call ζ_n a primitive nth root of 1 (or of unity) in E, and we have $E = F(\zeta_n)$.

Theorem 19. The Galois group $\mathrm{Gal}(E/F)$ is abelian. If $n = q$ is a prime (not $\mathrm{Char}(F)$), then $\mathrm{Gal}(E/F)$ is cyclic.

Proof. Let $\zeta = \zeta_n$ so that $E = F(\zeta)$. If $\sigma \in \mathrm{Gal}(E/F)$, then $\sigma(\zeta)$ is once again a root of $x^n - 1$. So there exists an $n_\sigma \in \mathbb{N}$ so that $\sigma(\zeta) = \zeta^{n_\sigma}$, with $1 \leq n_\sigma < n$. If $\tau \in \mathrm{Gal}(E/F)$, then also

$$\tau\sigma(\zeta) = \tau(\zeta^{n_\sigma}) = (\tau(\zeta))^{n_\sigma} = \zeta^{n_\tau n_\sigma},$$

so $n_{\tau\sigma} = n_\tau n_\sigma$ modulo n. Thus, we have a map $\sigma \mapsto n_\sigma$, and this gives us a homomorphism $\mathrm{Gal}(E/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$. Note that this is injective, since if $\sigma \neq \tau$, then $\sigma(\zeta) \neq \tau(\zeta)$, so $n_\sigma \neq n_\tau$. Therefore, $\mathrm{Gal}(E/F)$ is isomorphic to a subgrpup of $(\mathbb{Z}/n\mathbb{Z})^\times$, and hence it must be abelian.

Note that if n is prime, then $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic, so that $\mathrm{Gal}(E/F) \leq (\mathbb{Z}/n\mathbb{Z})^\times$ is also cyclic. □

4.2. **Noether's Equations.** Let E be a field, $G \subset \mathrm{Aut}(E)$ be a finite subgroup. Let $\sigma \mapsto \alpha_\sigma$ be a map $G \to E^\times$. The set of elements $\{\alpha_\sigma : \sigma \in G\}$ is called a *solution to Noether's equations* if

$$\alpha_\sigma \cdot \sigma(\alpha_\tau) = \alpha_{\sigma\tau}$$

for all $\sigma, \tau \in G$. We have the following criteria to determine whether something is a solution to Noether's equations.

Theorem 20 (Speiser)**.** The set $\{\alpha_\sigma : \sigma \in G\}$ is a solution to Noether's equations iff there exists $\beta \in E^\times$ such that

$$\alpha_\sigma = \frac{\beta}{\sigma(\beta)}$$

for all $\sigma \in G$.

Proof. ($\implies$): Assume that $\{\alpha_\sigma : \sigma \in G\}$ is a solution to Noether's equations. Since the automorphisms $\tau \in G$ are linearly independent over E, by Dedekind's independence of characters (**Theorem 7**), and the $\alpha_\tau \neq 0$, then there exists $\gamma \in E^\times$ such that

$$\sum_{\tau \in G} \alpha_\tau \tau(\gamma) \neq 0.$$

Let β be this element, i.e.,

$$\beta = \sum_{\tau \in G} \alpha_\tau \tau(\gamma) \neq 0.$$

Let σ be any element of G. If we apply σ to β, we have

$$\sigma(\beta) = \sum_{\tau \in G} \sigma(\alpha_\tau)\sigma\tau(\gamma).$$

If we multiply by α_σ, we obtain

$$a_\sigma \sigma(\beta) = \sum_{\tau \in G} \alpha_\sigma \sigma(\alpha_\tau)\sigma\tau(\gamma).$$

By Noether's equations, we have that $\alpha_\sigma(\sigma(\alpha_\tau)) = \alpha_{\sigma\tau}$, so we replace this to get

$$\alpha_\sigma \sigma(\beta) = \sum_{\tau \in G} \alpha_{\sigma\tau}\sigma\tau(\gamma).$$

Notice that $\sigma G = G$, so we can rewrite this as

$$\alpha_\sigma \sigma(\beta) = \sum_{\tau \in G} \alpha_\tau \tau(\gamma) = \beta.$$

Dividing by $\sigma(\beta)$, we have

$$a_\sigma = \frac{\beta}{\sigma(\beta)}.$$

($\Longleftarrow$): If we have a $\beta \in E^\times$ such that

$$\alpha_\sigma = \frac{\beta}{\sigma(\beta)}$$

for all $\sigma \in G$, then we see that

$$\alpha_\sigma \cdot \sigma(\alpha_\tau) = \frac{\beta}{\sigma(\beta)} \cdot \sigma\left(\frac{\beta}{\tau(\beta)}\right) = \frac{\beta}{\sigma(\beta)} \cdot \frac{\sigma(\beta)}{\sigma\tau(\beta)} = \frac{\beta}{\sigma\tau(\beta)} = \alpha_{\sigma\tau}.$$

□

Remark. In terms of group cohomology, Speiser's theorem says that $H^1(G, E^\times) = 1$. In other words, every 1-cocycle is a 1-coboundary.

We have an interesting situation when the α_σ actually live in the fixed field $F = E^G$ of G. In this case, let $\chi : G \to F^\times$ be given by $\chi(\sigma) = \alpha_\sigma$, with the $\{\alpha_\sigma\}$ solutions to Noether's equations. We claim that χ is a character of G with values in $F^\times$, since

$$\chi(\sigma\tau) = \alpha_{\sigma\tau} = \alpha_\sigma \sigma(\alpha_\tau) = \alpha_\sigma \alpha_\tau = \chi(\sigma)\chi(\tau),$$

where we critically use that $F = E^G$ to deduce $\sigma(\alpha_\tau) = \alpha_\tau$. Going backwards, we get that any character $\chi : G \to F^\times$ with $F = E^G$ defines a solution to Noether's equations.

Combining this observation with Speiser's Theorem, we obtain the first half of the following theorem.

Theorem 21. Let E/F be a Galois extension, $G = \mathrm{Gal}(E/F)$. Then for each character $\chi : G \to F^\times$, there exists $\beta \in E^\times$ such that

$$\chi(\sigma) = \frac{\beta}{\sigma(\beta)},$$

and conversely, if $\beta/\sigma(\beta) \in F$ for all $\sigma \in G$, then $\chi_\beta(\sigma) = \beta/\sigma(\beta)$ is a character of G.

Moreover, if r is the least common multiple of the orders of $\sigma \in G$, then $\beta^r \in F$.

Proof. Everything before the moreover has been shown. Thus, we just need to show that $\beta^r \in F$, where β defines a character χ as above. Noting that $F = E^G$, we just need to show that for all $\sigma \in G$, $\sigma(\beta^r) = \beta^r$. Notice that

$$\frac{\beta^r}{\sigma(\beta^r)} = \left(\frac{\beta}{\sigma(\beta)}\right)^r = \chi(\sigma)^r = \chi(\sigma^r) = \chi(e) = 1,$$

so $\beta^r = \sigma(\beta^r)$ for all $\sigma \in G$. Hence, $\beta^r \in F$. □

4.3. **Kummer Theory.** Kummer theory provides us with descriptions of field extensions which are obtained by adjoining nth roots. So Kummer theory actually gives us a characterization of abelian extensions in the presence of sufficient roots of unity.

Let F be a field containing n distinct nth roots of 1. Let $\mu_n(F)$ denote the group of distinct nth roots of 1 in F.

Definition. A *Kummer extensions* E of F is the splitting field of a polynomial

$$f(x) = (x^n - a_1)\cdots(x^n - a_r),$$

with $a_1, \ldots, a_r \in F$. In other words,

$$E = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r}).$$

Note that since F contains n distinct nth roots of 1, label these $\epsilon_1, \ldots, \epsilon_n$, then

$$x^n - a_i = \prod_{j=1}^{n}(x - \epsilon_j\alpha_i),$$

where $\alpha_i \in E$ with $\alpha_i^n = a_i$. Hence, $f(x)$ is separable, so E/F Galois extension, and we an realize $E = F(\alpha_1, \ldots, \alpha_r)$.

Let $\sigma \in G = \mathrm{Gal}(E/F)$. Then σ is completely determined by its action on the α_i, and

$$\sigma(\alpha_i) = \epsilon_{i,\sigma}\alpha_i,$$

since $\sigma(\alpha_i)$ is also a root of $x^n - a_i = 0$. If both $\sigma, \tau \in G$, then for each α_i we have

$$\begin{aligned}\tau\sigma(\alpha_i) = \tau(\epsilon_{i,\sigma}\alpha_i) &= \epsilon_{i,\sigma}\tau(\alpha_i) = \epsilon_{i,\sigma}\epsilon_{i,\tau}\alpha_i \\ &= \epsilon_{i,\tau}\epsilon_{i,\sigma}\alpha_i = \sigma\tau(\alpha_i).\end{aligned}$$

Hence, σ and τ commute on the generators of E/F, and hence $\mathrm{Gal}(E/F)$ is abelian.

Suppose $\sigma \in G$. Then for each α_i, we have

$$\begin{aligned}\sigma(\alpha_i) &= \epsilon_{i,\sigma}\alpha_i \\ \sigma^2(\alpha_i) &= \epsilon_{i,\sigma}^2\alpha_i \\ &\vdots \\ \sigma^k(\alpha_i) &= \epsilon_{i,\sigma}^k\alpha_i.\end{aligned}$$

Thus, if $\epsilon_{i,\sigma}$ has order $n_{i,\sigma}$ in the group $\mu_n(F)$, then $\sigma^{n_{i,\sigma}}(\alpha_i) = \alpha_i$. Since $\epsilon_{i,\sigma} \in \mu_n(F)$, a group of order n, we have that $n_{i,\sigma} \mid n$. Therefore,

$$\mathrm{ord}(\sigma) = \mathrm{lcm}_i\{n_{i,\sigma}\} = m_\sigma, \quad m_\sigma \text{ divides } n.$$

If we let $m = \mathrm{lcm}_{\sigma\in G}\{m_\sigma\}$, then m also divides n. This is the exponent of G by definition. Thus, we have proven the following result.

Theorem 22. If F contains n distinct nth roots of 1 and E is a Kummer extension of F, i.e., a splitting field of a polynomial

$$f(x) = (x^n - a_1) \cdots (x^n - a_r)$$

with $a_i \in F$, then

(a) E/F is a Galois extension.
(b) E/F is abelian (that is, $\mathrm{Gal}(E/F)$ is an abelian group).
(c) $\mathrm{Gal}(E/F)$ has exponent m dividing n.

As a corollary, we have the following.

Corollary 20. Let q be a prime and suppose F contains q distinct qth roots of 1. Let E be the splitting field of $x^q - a$ with $a \in F$. Then either $E = F$ and $x^q - a$ splits in F, or $x^q - a$ is irreducible and $\mathrm{Gal}(E/F)$ is cyclic of order q.

Proof. This is a consequence of (c) in the above theorem. We have that $\mathrm{Gal}(E/F)$ has exponent dividing the prime q. So it is either 1, in which case $\mathrm{Gal}(E/F)$ is trivial and $E = F$, or it is q, in which ase $(E : F) = q$, forcing $x^q - a$ to be irreducible. □

The interesting part of the above result is that it actually *completely* characterizes Kummer extensions. So an extension is Kummer iff (a), (b) and (c) hold. That is, we have the following.

Theorem 23. Let E/F be a field extension. We have E is a Kummer extension if and only if

(a) E/F is a Galois extension.
(b) E/F is abelian.
(c) $\mathrm{Gal}(E/F)$ has exponent m dividing n.

The goal will be to prove this theorem.

From here on out, we assume

- E/F is a Galois extension with $\mathrm{Gal}(E/F)$ abelian.
- If m is the exponent of $\mathrm{Gal}(E/F)$, then F contains m distinct mth roots of 1.

Let $\mu_m(F)$ denote the group of mth roots of 1 in F and let $G = \mathrm{Gal}(E/F)$. Let

$$\hat{G} = \{\chi : G \to \mu_m(F) \subset F^\times\}$$

be the set of characters of G with values in $\mu_m(F)$. Note that since G has exponent m, any character of G with values in $F^\times$ must take values in $\mu_m(F)$.

Claim 1. Since $m = \exp(G)$, the exponent of $G = \mathrm{Gal}(E/F)$, $\hat{G} \cong G$. Moreover, for any $\sigma \in G$, $\sigma \neq 1_G$, there exists a $\chi \in \hat{G}$ such that $\chi(\sigma) \neq 1_F$.

Proof. We drop the subscripts for G and F for the identity, since it should be clear from context which we are talking about.

We are assuming $\mathrm{Gal}(E/F) = G$ is abelian, so we can invoke the structure theorem for finite abelian groups to get

$$G \cong C_1 \times \cdots \times C_t$$

where C_i are cyclic groups of order m_i, with $m_1 \mid m_2 \mid \cdots \mid m_t = m$. Let σ_i denote the generator of C_i. From this, we see that any $\sigma \in G$ can be written as

$$\sigma = \sigma_1^{\nu_1} \cdots \sigma_t^{\nu_t},$$

with $\nu_i \pmod{m_i}$. Define a character $\chi_i : G \to \mu_m(F)$ by

$$\chi_i(\sigma_j) = \begin{cases} \epsilon_i \text{ if } j = i, \\ 1 \text{ if } j \neq i, \end{cases}$$

where we have ϵ_i is a primitive m_ith root of 1. Then if $\chi \in \hat{G}$, we can write $\chi(\sigma_i) = \epsilon_i^{\mu_i} = \chi_i(\sigma_i)^{\mu_i}$. This follows since σ_i has order m_i, and so $\chi(\sigma_i)$ must be an m_ith root of 1, so of the form $\epsilon_i^{\mu_i}$ for some $\mu_i \pmod{m_i}$. Thus, we see that we can write

$$\chi(\sigma) = \chi(\sigma_1^{\nu_1} \cdots \sigma_t^{\nu_t}) = \chi_1(\sigma_1)^{\mu_1\nu_1} \cdots \chi_t(\sigma_t)^{\mu_t\nu_t}.$$

Hence,

$$\chi = \chi_1^{\mu_1} \cdots \chi_t^{\mu_t}.$$

Conversely, every $\chi_1^{\mu_1} \cdots \chi_t^{\mu_t}$ defines a character of G. Thus, we see that we have

$$\hat{G} \cong \hat{C}_1 \times \cdots \times \hat{C}_t,$$

with $\hat{C}_t = \langle \chi_i \rangle \cong C_i$. So $\hat{G} \cong G$.

Now we show the moreover part. If $\sigma \in G$, then we write

$$\sigma = \sigma_1^{\nu_1} \cdots \sigma_t^{\mu_t}.$$

Since $\sigma \neq 1$, there is some $\nu_i \neq 0$, so

$$\chi_i(\sigma) = \epsilon_i^{\nu_i} \neq 1.$$

Thus, there exists a $\chi \in \hat{G}$ with $\chi(\sigma) \neq 1_F$. □

Noe, let

$$A = \{\alpha \in E^\times : \alpha^m \in F, m \text{ is the exponent of } G\}.$$

Then A is a multiplicative subgroup of $E^\times$ and $F^\times \subset A$. Let

$$A^m = \{\alpha^m : \alpha \in A\} \subset F^\times \qquad \text{and} \qquad F^{\times,m} = \{\alpha^m : \alpha \in F^\times\} \subset A^m.$$

There is a convenient way to calculate $G = \mathrm{Gal}(E/F)$.

Claim 2. (a) $A/F^\times \cong A^m/F^{\times,m}$.
(b) $A/F^\times \cong \hat{G} \cong G$.

Proof. (a) Consider the surjective mth power map $A \to A^m$ composed with the quotient map $A^m \to A^m/F^{\times,m}$. Let K be the kernel. We get an exact sequence

$$1 \to K \to A \to A^m/F^{\times,m} \to 1.$$

Note that

$$F^\times \subset K = \{\beta \in A : \beta^m \in F^{\times,m}\}.$$

Thus, if $\beta \in K$, then there exists $b^m \in F^{\times,m}$ such that $\beta^m = b^m$. So β is a root of the polynomial

$$x^m - b^m = 0.$$

Note that the roots of $x^m - b^m$ are $b, \epsilon_2 b, \ldots, \epsilon_m b$, where $1 = \epsilon_1, \epsilon_2, \ldots, \epsilon_m \in \mu_m(F)$ are the mth roots of 1 in F. Therefore, we get that $\beta = \epsilon_i b$ for some $\epsilon_i \in \mu_m(F)$. Thus, $\beta \in F^\times$. The choice of β was arbitrary, so we have that $K \subset F^\times$. Hence, $K = F^\times$. So

$$A/F^\times \cong A^m/F^{\times,m}$$

as desired.

(b) The goal here is to show $A/F^\times \cong \hat{G}$. So for every $[\alpha] \in A/F^\times$, we need to construct a character $\chi : G = \mathrm{Gal}(E/F) \to \mu_m(F)$. Fix $\alpha \in A$. For each $\sigma \in G$, consider $\alpha/\sigma(\alpha)$. Note that

$$\left(\frac{\alpha}{\sigma(\alpha)}\right)^m = \frac{\alpha^m}{\sigma(\alpha^m)}.$$

Recall that for $\alpha \in A$, we have that $\alpha^m \in F$ by the proof of (a), so $\sigma(\alpha^m) = \alpha^m$. Hence

$$\left(\frac{\alpha}{\sigma(\alpha)}\right)^m = 1.$$

So it is an mth root, an hence $\alpha/\sigma(\alpha) \in \mu_m(F) \subset F^\times$. We can define

$$\chi_\alpha : G \to \mu_m(F)$$

via

$$\chi_\alpha(\sigma) = \frac{\alpha}{\sigma(\alpha)}.$$

So we get a homomorphism $\theta : A \to \hat{G}$ with $\theta(\alpha) = \chi_\alpha$. This is indeed a homomorphism, since for each $\sigma \in G$ we have

$$\theta(\alpha\beta)(\sigma) = \chi_{\alpha\beta}(\sigma) = \frac{\alpha\beta}{\sigma(\alpha\beta)} = \frac{\alpha}{\sigma(\alpha)}\frac{\beta}{\sigma(\beta)} = \chi_\alpha(\sigma)\chi_\beta(\sigma) = \theta(\alpha)(\sigma)\theta(\beta)(\sigma),$$

so $\theta(\alpha\beta) = \theta(\alpha)\theta(\beta)$. We now note that every χ is of the form $\chi = \chi_\alpha$, as a consequence of Speisers theorem. The kernel will be

$$\mathrm{Ker}(\theta) = \{\alpha \in A : \chi_\alpha = 1\}.$$

Thus,

$$\mathrm{Ker}(\theta) = \left\{\alpha \in A : \frac{\alpha}{\sigma(\alpha)} = 1 \text{ for all } \sigma \in G\right\}.$$

Notice that if $\alpha \in \mathrm{Ker}(\theta)$, we have that $\alpha = \sigma(\alpha)$ for all $\sigma \in G$. This implies that α is in the fixed field, which means that $\alpha \in F^\times$. So $A/F^\times \cong \hat{G}$.

□

We are now ready to prove the theorem.

Proof of Theorem 23. The implication follows from what we showed earlier. It suffices to prove the other direction.
($\Longleftarrow$): Let $A = \{\alpha \in E^\times : \alpha^m \in F^\times\}$ again. Since we had $A/F^\times$ is a finite group by the claim prior, we can write

$$A = \alpha_1 F^\times \cup \cdots \cup \alpha_t F^\times$$

as the coset representation for $A/F^\times$. Note that

$$t = |A/F^\times| = |G| = (E : F)$$

again by the claim above.

Since $\alpha_i \in A$, we know that $\alpha_i^m = a_i \in F$ and α_i is a root of the polynomial

$$x^m - a_i \in F[x].$$

If $\mu_m(F) = \{\epsilon_1, \ldots, \epsilon_m\}$, then in $E[x]$ we have

$$x^m - a_i = \prod_{j=1}^{m}(x - \epsilon_j a_i).$$

Thus, $x^m - a_i$ splits completely in E.

We claim E is the splitting field of

$$\prod_{i=1}^{t}(x^m - a_i) \in F[x].$$

In other words, we claim that $E = F(\alpha_1, \ldots, \alpha_t)$. IF not, then $F \subset F(\alpha_1, \ldots, \alpha_t) \subset E$ is an intermediate field between E and F. So there exists some $\sigma \in G = \mathrm{Gal}(E/F)$ such that $\sigma \neq 1_G$,

but σ restricted to $F(\alpha_1, \ldots, \alpha_t)$ is the identity on the intermediate field. Now, there is a character $\chi \in \hat{G}$ such that $\chi(\sigma) \neq 1_F$. But $\hat{G} \cong A/F^\times$, that is, there is some $\alpha \in A$ so that $\chi = \chi_\alpha$. Thus,

$$\chi(\sigma) = \frac{\alpha}{\sigma(\alpha)} \neq 1,$$

so $\sigma(\alpha) \neq \alpha$ for this $\alpha \in A$. But we have

$$\alpha \in A = \alpha_1 F^\times \cup \cdots \cup \alpha_t F^\times.$$

Therefore $\alpha \in F(\alpha_1, \ldots, \alpha_t)$. This contradicts the fact that $\sigma(\alpha) \neq \alpha$, so we must have $E = F(\alpha_1, \ldots, \alpha_n)$. Thus, E is a Kummer extension of F. □

Specializing this to the case $m = q$ a prime, we get the following corollary.

Corollary 21. If E/F is Galois with $(E : F) = q$ a prime and F contains q distinct qth roots of 1, then E is the splitting field of an irreducible polynomial $x^q - a \in F[x]$.

We in fact have that if F contains m distinct mth roots of 1, then there is an order reversing bijection between subgroups N so that $F^{\times,m} \subset N \subset F^\times$ and abelian extensions E/F of exponent $m' \mid m$.

5. More on field extensions

5.1. **Simple Extensions.**

Definition. An extension E/F is said to be simple if E is generated over F by a single element. In other words, if $E = F(\alpha)$ for some $\alpha \in E$. The element α is then called the primitive element for E/F.

Example. If we adjoin $\sqrt{2}$ to $F = \mathbb{Q}$, we get that $E = \mathbb{Q}(\sqrt{2})$ is a simple extension of F.

The following theorem gives us a necessary and sufficient condition for a finite extension E/F to have a primitive element.

Theorem 24 (Steinitz)**.** Let E/F be a finite extension. Then E/F has a primitive element iff there are only a finite number if intermediate fields between F and E.

Proof. ($\Longrightarrow$) : Suppose $E = F(\alpha)$ so that it has a primitive element α. Let K be an intermediate field, so $F \subset K \subset E$. Let $f(x)$ be the minimal polynomial of α over F and $g(x)$ be the minimal polynomial of α over K. Then $g(x) \mid f(x)$ in $K[x] \subset E[x]$. Let K' be the subfield of E generated over F be the coefficients of $g(x)$. Since $g(x) \in K[x]$, we know $K' \subset K$, and $g(x)$ is also the minimal polynomial of α over K'. Now, $E = F(\alpha) = K(\alpha) = K'(\alpha)$, and $(E : K) = \deg(g) = (E : K')$. Since $K' \subset K \subset E$, we have that $(E : K') = (E : K)(K : K')$, so $(K : K') = 1$. In other words, $K = K'$.

This tells us that the intermediate fields $F \subset K \subset E$ are generated by the coefficients of the (monic) factors $g(x)$ of $f(x)$ in $E[x]$. Since there are only a finite number of such factors by the divisibility theory, there can only be a finite number of intermediate fields.

($\Longleftarrow$) : Now assume there are only finitely many intermediate fields $F \subset K \subset E$. If E and F are finite fields, then $E^\times$ is a cyclic group. If α is a generator so that $E^\times = \langle \alpha \rangle$, then $E = F(\alpha)$ and α is a primitive element. Thus, assume that E and F are infinite fields (if F finite, then E must be finite since the degree is finite, so we can rule this out, and likewise for the ridiculous claim E finite and F infinite). Let $E = F(\alpha_1, \ldots, \alpha_n)$, which we can do since E/F is finite. We will induct on n, the number of generators of E over F. For $n = 1$, we win, since α_1 is a primitive element. Assume $n = 2$, so $E = F(\alpha, \beta)$. Consider the intermediate fields $K_t = F(\alpha + t\beta)$, where $t \in F$. Then we have $F \subset K_t \subset E$.

The goal is to show that $E = K_t$ for some t. Since there are an infinite number of elements $t \in F$ (since F infinite by assumption), we must have that there is a pair $t_1 \neq t_2$ so that $K_{t_1} = K_{t_2}$. So $F(\alpha + t_1\beta) = F(\alpha + t_2\beta)$. Notice that this implies that

$$\beta = \frac{(\alpha + t_1\beta) - (\alpha + t_2\beta)}{t_1 - t_2} \in F(\alpha + t_1\beta),$$

since $(\alpha + t_2\beta) \in F(\alpha + t_1\beta)$. Notice as well that

$$\alpha = (\alpha + t_1\beta) - t_1\beta \in F(\alpha + t_1\beta).$$

Hence, $E = F(\alpha, \beta)$ (the smallest field generated by these elements) must be contained in K_{t_1}. But K_{t_1} is contained in E, so we have

$$E \subset K_{t_1} \subset E \implies E = K_{t_1} = F(\alpha + t_1\beta).$$

Hence, we have that $\alpha + t_1\beta$ is a primitive element.

The case for $n > 2$ follows inductively. Assume we can show it for $n-1$, then the goal is to show that $E = F(\alpha_1, \ldots, \alpha_n) = F(\alpha)$ for some α. Consider then

$$F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n).$$

We have that

$$F(\alpha_1, \ldots, \alpha_n) = F(\alpha')$$

by the induction hypothesis, so

$$F(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) = F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = F(\alpha')(\alpha_n) = F(\alpha', \alpha_n).$$

Now, by the $n = 2$ case, we have that

$$F(\alpha', \alpha_n) = F(\alpha)$$

for some α, so we get that $E = F(\alpha)$. Thus, the extension is primitive, and has primitive element $\alpha \in E$ for some suitable α. □

Notice that this covers the case of Galois extensions.

Corollary 22. If E/F is a finite separable extension, then there is a primitive element for E/F. In particular, finite Galois extensions are simple.

Proof. We have that E/F is a finite separable extension, so there is a basis $\omega_1, \ldots, \omega_n$ for E/F. Letting $f_i(x) \in F[x]$ be the minimal polynomial for ω_i over F, we have that

$$f(x) = f_1(x) \cdots f_n(x)$$

is separable. Let K be the splitting field of $f(x)$ over F. Then we have that $F \subset E \subset K$, and K/F is Galois.

We now invoke the Fundamental Theorem of Finite Galois Theory (**Theorem 13**) to get that the number of intermediate fields $F \subset K' \subset K$ is equal to the number of subgroups H of $G = \mathrm{Gal}(K/F)$, which is a finite group. So there are a finite number of intermediate fields for K/F, and since $E \subset K$, there are a finite number of intermediate fields for E and F. Thus, the last theorem tells us that E has a primitive element over F, as does K. □

5.2. **(Optional) Existence of Normal Basis.** We follow Artin [2] II N. Note that the following theorem is true for *any* field, thoguh we prove it only in the case where F contains infinite elements.

Theorem 25 (Existence of Normal Basis)**.** If E is a normal extension of F, and $\sigma_1, \ldots, \sigma_n$ are the elements of its group G, there is an element $\theta \in E$ such that the n elements $\sigma_1(\theta), \ldots, \sigma_n(\theta)$ are linearly independent with respect to F.

Proof. Recall that an extension E/F is normal if it is algebraic and every irreducible $p(x) \in F[x]$ which has a root $\alpha \in E$ splits completely in E. By **Theorem 24**, we have that there is a α such that $E = F(\alpha)$. Let $f(x)$ be the minimal polynomial for α, and put $\sigma_i(\alpha) = \alpha_i$. Then we set

$$g(x) = \frac{f(x)}{(x-\alpha)f'(\alpha)}$$

and

$$g_i(x) = \sigma_i(g(x)) = \frac{f(x)}{(x-\alpha_i)f'(\alpha_i)}.$$

We have that g_i is a polynomial in $E[x]$ having α_k as a root for $k \neq i$, and so in $E[x]/(f(x))$, we have

$$g_i(x)g_k(x) = 0 \text{ for } i \neq k.$$

Consider

$$g_1(x) + g_2(x) + \cdots + g_n(x) - 1 = 0.$$

The left side of the equation has degree at most $n-1$. Thus, the number of roots is at most $n-1$ unless it is identically 0; hence, if it is true for n different values, then it must be 0. Notice that

$$g_1(\alpha_1) + g_2(\alpha_1) + \cdots + g_n(\alpha_1) = \sigma_1(g(\alpha_1)) + \cdots + \sigma_n(g(\alpha_n)).$$

Notice that if $i = k$, then we have that $\sigma_i(g(\alpha_k)) = g_k(\alpha_k) = 1$, and if $i \neq k$¡ then $\sigma_i(g(\alpha_k)) = 0$. Hence, we have

$$g_1(\alpha_1) + g_2(\alpha_1) + \cdots + g_n(\alpha_1) = 1$$

or

$$g_1(\alpha_1) + g_2(\alpha_1) + \cdots + g_n(\alpha_1) - 1 = 0.$$

The same applies for $\alpha_2, \ldots, \alpha_n$, so we get that we must have that the left hand side is identically zero; i.e., we have

$$g_1(x) + g_2(x) + \cdots + g_n(x) - 1 = 0.$$

Multiplying the above by $g_i(x)$ and using the fact that $g_i(x)g_k(x) = 0 \pmod{f(x)}$, we get

$$(g_i(x))^2 = g_i(x) \pmod{f(x)}.$$

Computing the determinant, we see that

$$D(x) = |\sigma_i\sigma_k(g(x))| \text{ for } i, k = 1, \ldots, n.$$

The goal is to show that $D(x) \neq 0$. Squaring it and computing its value mod $f(x)$, we see that from the prior discussion the determinant has 1 along the diagonal and zero elsewhere when we look modulo $f(x)$. Thus,

$$(D(x))^2 = 1 \pmod{f(x)}.$$

Now, $D(x)$ is a polynomial which can only have a finite number of roots in F. Avoiding them, we can find a value a for x such that $D(a) \neq 0$. Setting $\theta = g(a)$, we have that

$$|\sigma_i\sigma_k(\theta)| \neq 0.$$

Now, consider any linear relation

$$x_1\sigma_1(\theta) + \cdots + x_n\sigma_n(\theta) = 0,$$

where $x_i \in F$. Applying σ_i to it leads to n homogeneous equations for the n unknowns x_i. The fact that $|\sigma_i \sigma_k(\theta)| = 0$ implies that $x_i = 0$, and so the theorem is established. □

5.3. **(Optional) Solutions of Equations by Radicals.** We briefly mentioned solutions by radicals in the Preliminaries section. We elaborate on this now, following Artin [2].

Definition. If E/F is an extension of fields, we call it an extension by radicals if there exists intermediate fields $B_1, B_2, \ldots, B_r = E$ and $B_i = B_{i-1}(\alpha_i)$, where each α_i is a root of an equation of hte form $x^{n_i} - a_i = 0$, $a_i \in B_{i-1}$.

A polynomial $f(x)$ in a field F is said to be solvable by radicals if its splitting field lies in an extension by radicals.

Unless otherwise stated, we assume that the base field has characteristic 0, and that F contains as many roots of unity as are needed to make the subsequent statements valid.

Note that any extension of F by radicals can always be extended to an extension of F by radicals which is normal over F. So if $B_1 = B_0(\alpha_1)$ is an extension by radicals, then we have that B_1 is a normal extension as well, since it contains not only α_1 but $\epsilon\alpha_1$ for any n_1-root of unity ϵ. Thus, B_1 is the splitting field of $x^{n-1} - a_1$. If

$$f_1(x) = \prod_{\sigma \in \mathrm{Gal}(B_1/B_0)} (x^{n_2} - \sigma(a_2)),$$

then $f_1 \in B_0[x]$, and adjoining successively the roots of $x^{n_2} - \sigma(a_2)$ brings us to an extension of B_2 which is normal over F. Continuing in this way, we arrive at an extension of E by radicals which will be normal over F.

We recall briefly a group G is solvable if it has a sequence of subgroups

$$1 = G_0 \leq G_1 \leq \cdots \leq G_k = G$$

where $G_{n-1} \trianglelefteq G_n$ and G_n/G_{n-1} is an abelian group for $n = 1, \ldots, k$.

Theorem 26. Let K be the splitting field for $f(x) \in F[x]$. The polynomial $f(x)$ is solvable by radicals if and only if $\mathrm{Gal}(K/F)$ is solvable.

Sketch of Proof. ($\Longrightarrow$) : Assume $f(x)$ is solvable by radicals. Let E be a normal extension of F by radicals containing the splitting field K of $f(x)$. Let $G = \mathrm{Gal}(E/F)$. For each i we have that B_i is a Kummer extension of B_{i-1}, so the group B_i/B_{i-1} is abelian. Thus, letting $G_{B_n} = \mathrm{Gal}(E/B_n)$, we get

$$1 = G_{B_k} \leq G_{B_{k-1}} \leq \cdots \leq G_{B_0} = G$$

is a normal sequence where the quotients are abelian, and hence G is solvable. Labeling $G_K = \mathrm{Gal}(E/K)$, we see that $G/G_K = \mathrm{Gal}(E/F)/\mathrm{Gal}(E/K) \cong \mathrm{Gal}(K/F)$, so $\mathrm{Gal}(K/F)$ is the homomorphic image of a solvable group, hence solvable.
($\Longleftarrow$) : Suppose $\mathrm{Gal}(K/F)$ is solvable. Let E be the splitting field of $f(x)$. Let

$$1 = G_r \subset \cdots \subset G_1 \subset G_0 = G = \mathrm{Gal}(K/F)$$

be a solvable sequence. Label B_i to be the fixed field associated to G_i. Since G_{i-1} is the group $\mathrm{Gal}(E/B_{i-1})$, and the group G_{i-1}/G_i is abelian, then B_i is a Kummer extension of B_{i-1}, hence an extension by radicals. Thus, E is an extension by radicals. □

5.4. **The Algebraic Closure of a Field.** The notes now shift to following Jacobson [1].

Definition. A field L is called algebraically closed if every polynomial $f(x) \in L[x]$ of degree ≥ 1 has a root in L.

Lemma 11. Let L be an algebraically closed field.
(1) If $f(x) \in L[x]$, then $f(x)$ splits completely into linear factors in $L[x]$.

(2) If F is a subfield of L, then every polynomial $f(x) \in F[x]$ has a root in L, and in fact splits completely in $L[x]$.

Proof. (1) Write $f(x) = f_1(x) \cdots f_r(x)$, the product of its irreducible factors. Notice that $f_i(x) \in L[x]$ is a polynomial of degree ≥ 1, so it has a root in L (by definition). Since $f_i(x)$ is irreducible, it cannot be factored any further, and so it must be a linear factor. Hence, $f_i(x)$ is a linear factor with respect to its root, so $f(x)$ splits completely into linear factors.

(2) We have $f(x) \in F[x] \subset L[x]$, so viewing it in $L[x]$ we have that it splits completely into linear factors by (1). Thus, it has a root in L.

□

The first basic fact towards the existence of an algebraic closure is the following.

Theorem 27. Let F be a field. Then there exists an algebraically closed field L such that $F \subset L$.

Proof. We proceed in two steps. In the first step, we construct an extension E_1/F such that every polynomial $f(x) \in F[x]$ of degree ≥ 1 has a root in E_1. To do this, we associate to every $f(x) \in F[x]$ with $\deg(f) \geq 1$ an indeterminate, labeled x_f. Let

$$S := \{x_f : f(x) \in F[x], \deg(f) \geq 1\}.$$

Let $R = F[S]$ be the polynomial ring in this infinite number of variables. Let

$$\mathfrak{a} = \langle f(x_f) : f(x) \in F[x], \deg(f) \geq 1 \rangle \subset R$$

be an ideal generated by the $f(x_f)$.

The first claim is that $\mathfrak{a}$ is non-trivial. If $1 \in \mathfrak{a}$, then there is an expression

$$1 = g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n})$$

in R, that is, with coefficients $g_i \in R$. Set $x_i = x_{f_i}$ for notational simplicity. Let $x_{n+1}, \ldots, x_N$ be any remaining variables occurring in $g_1, \ldots, g_n$. Then we have

$$1 = g_1(x_1, \ldots, x_N) f_1(x_1) + \cdots + g_n(x_1, \ldots, x_N) f_n(x_n)$$

in $F[x_1, \ldots, x_n] \subset R$.

Now take a finite extension E'/F in which each polynomial $f_1(x), \ldots, f_n(x)$ has a root, labeling these $\alpha_1, \ldots, \alpha_n$. Take $\beta_{n+1}, \ldots, \beta_N$ to be any elements in E'. Then we have a non-trivial homomorphism

$$T : F[x_1, \ldots, x_N] \to E'$$

sending

$$T(x_i) = \alpha_i \text{ for } 1 \leq i \leq n, \quad T(x_i) = \beta_i \text{ for } n+1 \leq i \leq N.$$

The relation

$$1 = g_1 f(x_1) + \cdots + g_n f(x_n)$$

in $F[x_1, \ldots, x_N]$ becomes $1 = 0$ in E' after applying this map, since

$$T(1) = 1 = T(g_1 f(x_1)) + \cdots + T(g_n f(x_n))$$
$$= g_1(\alpha_1, \ldots, \alpha_n, \beta_{n+1}, \ldots, \beta_N) f(\alpha_1) + \cdots + g_n(\alpha_1, \ldots, \alpha_n, \beta_{n+1}, \ldots, \beta_N) f(\alpha_n) = 0.$$

This is a contradiction, so $\mathfrak{a}$ is a non-trivial ideal of R.

Now, let $\mathfrak{m}$ be a maximal ideal of R containing $\mathfrak{a}$. Consider $E_1 = R/\mathfrak{m}$. Since $\mathfrak{m}$ is maximal, E_1 is a field, and we have $F \subset E_1$. Moreover, each $f(x) \in F[x]$ has a root in E_1, namely $\overline{x_f} = x_f + \mathfrak{m}$.

In step 2, the goal is to build our algebraically closed field L. We inductively construct a tower of fields

$$F = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_k \subset \cdots$$

such that every polynomial $g(x) \in E_i[x]$ of degree $\deg(g) \geq 1$ has a root in E_{i+1}.

Let

$$L = \bigcup_{i=0}^{\infty} E_i.$$

Then L is a field, since it is an increasing nested union of fields. The claim is that L is algebraically closed.

Let $f(x) \in L[x]$, and write

$$f(x) = \sum_{i=0}^{m} a_i x^i,$$

with $m = \deg(f) \geq 1$. Then there is a field in our tower, say without loss of generality E_k, such that the coefficients $a_0, \ldots, a_m \in E_k$. Then we have that $f(x) \in E_k[x]$, so $f(x)$ has a root in $E_{k+1} \subset L$. Thus, L is algebraically closed and contains F. □

We now have the tools to define the algebraic closure of a field.

Definition. If F is a field, then an algebraic closure of F is a field, denoted $\overline{F}$, such that

(i) $\overline{F}$ is algebraic over F.
(ii) $\overline{F}$ is algebraically closed.

Thus, we see the following corollary.

Corollary 23. If F is a field, then F admits an algebraic closure $\overline{F}$.

Proof. Take $F \subset L$ as in the theorem, with L algebraically closed. Set

$$\overline{F} = \{y \in L : y \text{ is algebraic over } F\}.$$

There are two facts we need to show:

(1) $\overline{F}$ is a field. If $a, b \in \overline{F}$, then $F(a, b)$ is a finite extension of F, so

$$a \pm b, a \cdot b, a/b \in F(a, b) \subset \overline{F}$$

and so are algebraic over F.

(2) $\overline{F}$ is algebraically closed. To see this, if $f(x) \in \overline{F}[x]$, then since $\overline{F} \subset L$, $f(x)$ has a root in L. We now write out f;

$$f(x) = \sum_{j=0}^{m} a_j x^j.$$

Notice this is of degree $m \geq 1$, and each $a_j \in \overline{F}$, so it is algebraic over F. Then $F(a_0, \ldots, a_m)$ is a finite algebraic extension of F. Letting $\xi \in L$ be a root of $f(x) = 0$, then since $f(x) \in F(a_0, \ldots, a_m)[x] \subset \overline{F}[x]$, ξ is algebraic over $F(a_0, \ldots, a_m)$. Then the degree $(F(a_0, \ldots, a_m, \xi) : F(a_0, \ldots, a_m)) < \infty$ implies $(F(a_0, \ldots, a_m, \xi) : F) < \infty$, which in turn implies ξ is algebraic over F, so $\xi \in \overline{F}$ by definition.

□

The goal now is to determine whether algebraic closures are unique up to isomorphism. For this, we need an extension of a previous result extending field homomorphisms.

Theorem 28. Let F be a field, E an algebraic extension of F, and $\sigma : F \hookrightarrow L$ an embedding of F into an algebraically closed field L. Then there exists an extension of σ to an embedding $\tau : E \hookrightarrow L$.

Proof. This is a Zorn's lemma argument. Let

$$S = \{(K, \tau) : F \subset K \subset E \text{ and } \tau : K \hookrightarrow L \text{ extends } \sigma\}.$$

We have that S is non-empty, since $(F, \sigma) \in S$. Put a partial ordering on S via

$$(K, \tau) < (G, \kappa) \text{ iff } K \subset G \text{ and } \kappa|_K = \tau.$$

We now need to show that all chains are bounded. Let $(K_1, \tau_1) < \cdots < (K_n, \tau_n) < \cdots$ be an increasing chain in S. Notice that we can set $K = \bigcup_n K_n$, which is a field, and we have that $F \subset K \subset E$. We can also set τ to be the unique homomorphism such that $\tau|_{K_i} = \tau_i$. Note this is well-defined by the ordering (i.e. by inclusion). We have that (K, τ) is an upper bound of our chain, so Zorn's lemma says that we have a maximal element in S, denote it by (K, τ).

The claim then is that $K = E$. If not, we have $\alpha \in E \setminus K$. Note that α is algebraic over F, since E/F is algebraic, and since $F \subset K$, we have α is algebraic over K. By prior results (**Theorem ??**) we can extend $\tau : K \hookrightarrow L$ to $\tau' : K(\alpha) \hookrightarrow L$. Note this contradicts maximality, and so $K = E$. □

Corollary 24. Let E be an algebraic closure of F, L an algebraically closed field, and $\sigma : F \hookrightarrow L$. Suppose L is algebraic over $\sigma(F)$. Then $E \cong L$.

Proof. Let $\sigma : F \hookrightarrow L$. By our theorem, this extends to $\tau : \overline{F} = E \hookrightarrow L$. We have that L is algebraic over $\sigma(F)$, and this implies that L is algebraic over $\tau(E)$. We have $\tau(E)$ is algebraically closed, so $L = \tau(E)$. In other words, $L \cong E$. □

We have now the desired result.

Corollary 25. If E and E' are both algebraic closures of F, then $E \cong E'$.

One question to ask is how large is the algebraic closure of a field?

Lemma 12. (1) If F is infinite, then the cardinality of the algebraic closure is the same as the field.
(2) If F is finite, the cardinality of the algebraic closure is countable.

(1) If F is infinite, we have that $|\overline{F}| = |F|$. To see this, notice that we can write

$$\overline{F} = F \cup \left(\bigcup_{n \geq 1} \bigcup_{\deg(f) = n} Z(f) \right),$$

where $Z(f)$ is the set of roots $f(x) = 0$ in $\overline{F}$. Since $|Z(f)| \leq n = \deg(f)$ and $|\{f(x) \in F[x] : \deg(f) = n\}| = |F^{n+1}| = |F|$, where we deduce the first equality from looking at the coefficients of the polynomial, then

$$\left| \bigcup_{\deg(f) = n} Z(f) \right| = |F|$$

and so

$$\left| \bigcup_{n} \bigcup_{\deg(f) = n} Z(f) \right| = |F|.$$

(2) If F is finite, then the same argument gives us that $|\overline{F}| \leq |\mathbb{Z}|$, so that $\overline{F}$ is countable.

A consequence of (1) is the following.

Corollary 26. We have that $\overline{\mathbb{Q}} \neq \mathcal{C}$.

5.5. **Separability, Normality, and Galois Extensions.** The goal here is to investigate the concepts of separability, normality, and Galois extensions in the context of infinite extensions (as opposed to the finite results which we have discovered). Throughout, we fix a field F and we denote its algebraic closure by $\overline{F}$. If E/F is any algebraic extension, we view $E \subset \overline{F}$, so that $\overline{F}$ is also the algebraic closure of E.

We first generalize our definition of a splitting field.

Definition. Let $\Gamma = \{f(x) \in F[x] : \deg(f) \geq 1\} \subset F[x]$ be a collection of polynomials. An extension E/F is called a splitting field of Γ if:

(1) Every $f(x) \in \Gamma$ splits completely into linear factors in $E[x]$, and
(2) $E = F(\{\alpha : f(\alpha) = 0 \text{ for some } f(x) \in \Gamma\})$.

Note that $\overline{F}$ is the splitting field of the family $\Gamma = F[x]$.

Zorn's lemma lets us extend the uniqueness of splitting fields to families, as seen in the next theorem.

Theorem 29. Let $\sigma : F \to F'$ be an isomorphism of fields, $\Gamma \subset F[x]$, and $\Gamma' = \sigma(\Gamma) \subset F'[x]$ the corresponding family of polynomials over F'. If E/F is a splitting field of Γ and E'/F' a splitting field of Γ', then σ extends to an isomorphism $\tau : E \to E'$.

The proof of this is essentially the same as **Theorem 28**, so we omit it.

Definition. We define

$$\mathrm{Aut}(E/F) = \{\sigma : E \to E : \sigma \text{ is an automorphism}, \sigma|_F = \mathrm{id}_F\}.$$

Corollary 27. If E is the splitting field (in $\overline{F}$) of a family of monic polynomials $\Gamma \subset F[x]$ and $\sigma \in \mathrm{Aut}(\overline{F}/F)$, then $\sigma : \Gamma \to \Gamma$ and so restricts to an element of $\mathrm{Aut}(E/F)$.

Recall that an algebraic extension E/F is said to be normal if any irreducible polynomial $f(x) \in F[x]$ which has a root in E splits completely into linear factors in $E[x]$.

Lemma 13. If E is a normal extension of F, then E is a splitting field of a family Γ.

Proof. Consider

$$\Gamma_E := \{p_\alpha(x) \in F[x] : p_\alpha \text{ is the minimal polynomial in } F[x] \text{ for all } \alpha \in E\}.$$

Notice that for all $p_\alpha \in \Gamma_E$, we can view $p_\alpha(x) \in E[x]$, and we see that, since E is normal, $p_\alpha(x)$ splits into linear factors. Next, we need to show that

$$E = F(\{\alpha : f(\alpha) = 0 \text{ for some } f(x) \in \Gamma\}).$$

However, this follows just from definitions. That is, this is the smallest field so that every polynomial in $F[x]$ splits into linear factors in $E[x]$. □

The next result is a converse.

Theorem 30. If E is the splitting field over F for a set of monic polynomials $\Gamma \subset F[x]$, then E is normal over F.

Proof. Let $f(x) \in F[x]$ be irreducible and have a root in E. In $\overline{F}[x]$, we have

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i)$$

with $\alpha = \alpha_1 \in E$. The goal is to show that for all i, $\alpha_i \in E$. If this is the case, then $f(x)$ splits completely into linear factors in $E[x]$, and so by definition E is a normal extension of F.

Consider $E(\alpha_i)$. Since E is a splitting field over F for the family Γ, we know that $F(\alpha_i) \subset E(\alpha_i)$ is a splitting field for the same family Γ. Note that α and α_i have the same irreducible minimal polynomial, $f(x)$, so we have that

$$F(\alpha) \xrightarrow{\cong} F[x]/(f(x)) \xrightarrow{\cong} F(\alpha_i).$$

Thus, we have an isomorphism $\sigma : F(\alpha) \to F(\alpha_i)$. Since $E(\alpha)$ is the splitting field of Γ over $F(\alpha)$ and $E(\alpha_i)$ is the splitting field of Γ over $F(\alpha_i)$, then by **Theorem 29** we see that σ extends to an isomorphism $\tau : E(\alpha) \to E(\alpha_i)$. Since $\sigma|_F = \mathrm{id}_F$, we have $\tau|_F = \mathrm{id}_F$. Since E is the splitting field over F of $\Gamma \subset F[x]$, the isomorphism τ "stabilizes" E; in other words, $\tau(E) = E$. Since $\alpha \in E$, we have that $E(\alpha) = E$, so $E(\alpha_i) = \tau(E(\alpha)) = \tau(E) = E$. Hence, $\alpha_i \in E$ for all i. □

We now move on to the normal closure.

Definition. Let E/F be an algebraic extension, $F \subset E \subset \overline{F}$. Let K be the splitting field over F of the family

$$\Gamma_E = \{f_\alpha(x) : \alpha \in E, f_\alpha(x) \in F[x] \text{ the minimal polynomial of } \alpha\}.$$

We call K the normal closure of E.

Notice a few facts about K based on the definition:

- $E \subset K$,
- K is a normal extension of F,
- K is the smallest normal extension of F containing E and contained in $\overline{F}$.

The name "normal closure" makes sense based off of these.

Definition. An algebraic extension E/F is called Galois if E is normal and separable over F.

Note here that E/F is allowed to be an infinite extension. If E/F is a finite extension, then this recovers the definition of Galois from before (see **Theorem 12**). Note as well that the definition of separability doesn't care whether the extension is finite or infinite.

If E/F is a Galois extension, then we set

$$\mathrm{Gal}(E/F) := \mathrm{Aut}(E/F) = \{\sigma \in \mathrm{Aut}(E) : \sigma|_F = \mathrm{id}_F\}.$$

As before, we get the following result.

Proposition 4. Let E/F be a Galois extension and $G := \mathrm{Gal}(E/F)$. Then $F = E^G$.

Proof. Let E/F be Galois. By definition, $F \subset E^G$. Suppose that $E^G \neq F$, so that there is some $\alpha \in E^G \setminus F$. We can view $F \subset E \subset \overline{F}$, since E is algebraic over F, so $\alpha \in \overline{F}$. Since E/F is separable, we have that the minimal polynomial for α, denoted $p_\alpha \in F[x]$, is also separable. In $\overline{F}[x]$, we have that it splits;

$$p_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_r)$$

where we set $\alpha_1 = \alpha$. Since $F(\alpha) \cong F[x]/(p_\alpha(x)) \cong F(\alpha_2) \subset \overline{F}$, we get an embedding

$$\sigma : F(\alpha) \hookrightarrow \overline{F}$$

such that $\sigma(\alpha) = \alpha_2 \neq \alpha$ (the $\neq$ comes from the fact that p_α is separable).

Since E/F is algebraic, then by **Theorem 28** we have that σ extends to an embedding $\tau : E \to \overline{F}$, again with $\tau(\alpha) = \alpha_2$. Since E/F is a normal extension, it is the splitting field of some family $\Gamma \subset F[x]$ by **Lemma 13**, and the corollary of uniqueness of splitting fields (**Corollary 27**) gives $\tau(E) = E$; that is, $\tau \in G = \mathrm{Gal}(E/F)$. But $\tau(\alpha) = \sigma(\alpha) = \alpha_2 \neq \alpha$. So we have an element $\tau \in G$ which does not fix α, contradicting $\alpha \in E^G$. □

6. Infinite Galois Theory

The Galois theory of infinite algebraic extensions is due to Krull. Krull constructs the Galois group of an infinite algebraic extension as a profinite group, and the topology of the Galois group plays a definitive role. So we need to start by exploring topological groups.

6.1. **Topological Groups.**

Definition. A topological group is a group G with a topology such that the maps

$$G \times G \to G \text{ given by } (x, y) \mapsto x \cdot y,$$

$$G \to G \text{ given by } x \mapsto x^{-1}$$

are continuous. In other words, multiplication and inversion are continuous.

We list some common facts about topological groups.

Lemma 14. Any open subgroup H of a topological group G is also closed.

Proof. We begin by writing G in terms of its coset decomposition; so we have

$$G = \bigsqcup gH.$$

Note that we have that the map $\theta_g : G \to G$ given by $\theta_g(x) = gx$ is a homeomorphism; it is continuous (since multiplication is continuous), it is invertible (with inverse given by $\theta_{g^{-1}}$), and its inverse is continuous. To see the last remark, note that

$$\theta_{g^{-1}}(x) = g^{-1}x = (x^{-1}g)^{-1},$$

so it is the composition of the inverse map, along with multiplication on the right, along with the inverse map again, so it is continuous. Hence, θ_g is a homeomorphism, so in particular an open map. Thus, $gH = \theta_g(H)$ is an open set for each g. Thus, we can realize H as

$$H = G \setminus \bigsqcup_{g \neq e} gH;$$

by what we've shown, this is the complement of an open set, hence closed. □

Lemma 15. Any closed subgroup of H of finite index is also open.

Proof. Since it is finite index, we have that

$$G = \bigsqcup_{i=1}^{n} g_i H.$$

By what we've shown, we know that $g_i H$ is a closed set for all i. Without loss of generality, assume $g_1 = e$. Then we get that

$$G \setminus \bigsqcup_{i=2}^{n} g_i H = \bigcap_{i=1}^{n} (g_i H)^c = H.$$

This is a finite intersection of open sets, hence open. Thus, H is also open. □

Lemma 16. Let H, U be subgroups of G, and assume that U is open. If $U \subset H$, then H is open.

Proof. We write H in terms of its coset decomposition with respect to U. So we have

$$H = \bigsqcup hU.$$

Multiplication by $h \in H \subset G$ is a homeomorphism, so H is an arbitrary union of open sets, hence open. □

Let G be a topological group with identity e. We claim that e has a fundamental system of neighborhoods $\mathfrak{R} = \mathfrak{R}(e)$ which satisfies the following:

(1) For all $U \in \mathfrak{R}$, $e \in U$.
(2) If $U_1, U_2 \in \mathfrak{R}$, then $U_1 \cap U_2 \in \mathfrak{R}$.
(3) For all $U \in \mathfrak{R}$, there exists $W \in \mathfrak{R}$ such that $W \cdot W \subset U$.
(4) For all $U \in \mathfrak{R}$, $U^{-1} \in \mathfrak{R}$.
(5) For all $U \in \mathfrak{R}$, there exists $W \in \mathfrak{R}$ such that $W \subset gUg^{-1} \in \mathfrak{R}$.

Remark. If a group G possesses a set $\mathfrak{R}$ of subsets of G satisfying these properties, then G can be givne the structure of a topological group with $\mathfrak{R}$ a fundamental system of neighborhoods of e.

If $g \in G$, then a fundamental system of neighborhoods of g are the gU with $U \in \mathfrak{R}$. In other words, we get

$$\mathfrak{R}(g) = \{gU : U \in \mathfrak{R}(e)\}.$$

So we translate around the fundamental system of neighborhoods.

6.2. **Galois Groups.** Let E/F be a Galois extension. Thus, E is a separable, normal, algebraic extension of F. Let $G = \mathrm{Gal}(E/F)$. Let

$$\mathfrak{K} := \{K_\lambda : F \subset K_\lambda \subset E \text{ with } K_\lambda/F \text{ a finite Galois extension}\}$$

with parameter set $\lambda \in \Lambda$. For each K_λ, E/K_λ is still a Galois extension, and if we set $N_\lambda = \mathrm{Gal}(E/K_\lambda)$, then N_λ is a normal subgroup of G and $\mathrm{Gal}(K_\lambda/F) = G/N_\lambda$. The argument for both of these claims is the same as for finite Galois theory.

Let $\mathfrak{R} = \{N_\lambda = \mathrm{Gal}(E/K_\lambda) : \lambda \in \Lambda\}$.

Proposition 5. We have that $\mathfrak{R}$ can be taken as a fundamental system of neighborhoods of e for a topology on G.

Proof. We verify the properties.

(1) It is clear that $e \in N_\lambda$ for all λ.
(2) If $N_\lambda, N_\mu \in \mathfrak{R}$, then we claim that there is a N_ν so that $N_\lambda \cap N_\mu = N_\nu \in \mathfrak{R}$. To see this, let $K_\nu = K_\lambda \cdot K_\mu$ be the composite field. Then we have that K_ν/F is finite Galois, and $N_\nu = \mathrm{Gal}(E/K_\nu) = N_\lambda \cap N_\mu$.
(3) For all $N_\lambda \in \mathfrak{R}$, there exists an N_μ such that $N_\mu \subset N_\mu \subset N_\lambda$ (to see this, let $N_\mu = N_\lambda$).
(4) For all $N_\lambda \in \mathfrak{R}$, there exists an N_μ so that $N_\mu^{-1} = N_\lambda$ (to see this, take $N_\mu = N_\lambda$).
(5) For all $N_\lambda \in \mathfrak{R}$ and $\sigma \in G$, there exists N_μ such that $\sigma N_\mu \sigma^{-1} = N_\lambda$ (N_λ is normal, so take $N_\mu = N_\lambda$).

□

Using our remark, we get a topology on $G = \mathrm{Gal}(E/F)$, called the Krull topology. We now list some basic facts on the Krull topology.

Lemma 17. The Krull topology is T_0; that is, given $\sigma, \tau \in G$ with $\sigma \neq \tau$, there exists a neighborhood V of σ such that $\tau \notin V$.

Proof. We remark that, since $E = \bigcup_\lambda K_\lambda$, $\{e\} = \bigcap_\lambda N_\lambda$. We can then shift this around to get $\{\sigma\} = \bigcap_\lambda \sigma N_\lambda$. Hence, there exist a λ such that $\tau \notin \sigma N_\lambda$ (since otherwise it would be in this intersection). Take $V = \sigma N_\lambda$ and we have the desired result. □

Remark. Since σN_λ is both open and closed, we get that G is totally disconnected.

Lemma 18. The Krull topology on G is Hausdorff.

Proof. Take $\sigma, \tau \in G$, $\sigma \neq \tau$. Since these are distinct, there exists a finite Galois extension K/F such that $\sigma|_K \neq \tau|_K$. Let $K = K_\lambda$. We have that $\sigma(N_\lambda) \neq \tau(N_\lambda)$; since these are distinct cosets of N_λ in G, we get that $\sigma N_\lambda \cap \tau N_\lambda = \varnothing$. □

Lemma 19. For all $\sigma \in G$, $\{\sigma\}$ is closed.

Proof. All of the N_λ are both open and closed. The fact that they are open follows by construction of the Krull topology, and the fact that they are closed follows since they have finite index in G. Now,

$$\{\sigma\} = \bigcap_\lambda \sigma N_\lambda,$$

so it is an arbitrary intersection of closed sets; hence, it is closed. □

Lemma 20. If E/F is finite, then the Krull topology is the discrete topology.

Proof. Apriori, we have that singleton sets are closed, so it suffices to show that they are open. But since the extension is finite, we can use **Lemma 15** to get that these are also open. Hence, singletons are open and closed, so the topology is discrete. □

We now characterize the open subgroups of the Galois group.

Proposition 6. Let $G = \mathrm{Gal}(E/F)$, equipped with the Krull topology. Then $H \subset G$ is an open subgroup iff there exists $F \subset K \subset E$ with $(K : F) < \infty$ such that $H = \mathrm{Gal}(E/K)$.

Proof. ($\implies$) : Suppose H is an open subgroup of G. H is a subgroup, so $e \in H$, and hence there exists a $\lambda \in \Lambda$ such that $N_\lambda \subset H$. Thus, $(G : H) \leq (G : N_\lambda) < \infty$. Now, $N_\lambda = \mathrm{Gal}(E/K_\lambda)$ is a normal subgroup of G, so we have $\mathrm{Gal}(K_\lambda/F) = G/N_\lambda$ is finite and $H/N_\lambda \subset G/N_\lambda$. By the finite Galois correspondence, there is an intermediate field $F \subset K \subset K_\lambda$ so that $\mathrm{Gal}(K_\lambda/H) = H/N_\lambda$. Thus, $H = \mathrm{Gal}(E/K)$.
($\impliedby$): If K/F is finite, we have that K is separable over F. This follows since $K \subset E$ and E is separable. Let L be the normal closure of K. Then L/F is finite Galois, so $L = K_\lambda$ for some λ. Hence, $N_\lambda \subset H$. Since $H \subset G$ and N_λ is open, we have that H is open by **Lemma 16**. □

The next goal is to characterize the closed subgroups of the Galois group.

Proposition 7. Let $G = \mathrm{Gal}(E/F)$ with the Krull topology. Then H is a closed subgroup of G iff there exists a collection $\{U_\alpha : \alpha \in A\}$ of open subgroups such that $H = \bigcap_\alpha U_\alpha$.

Before proving this, we have a useful lemma.

Lemma 21. Let H be any subgroup of G. Then its closure $\overline{H}$ is given by

$$\overline{H} = \bigcap_\lambda H N_\lambda.$$

Proof. By definition of the closure, we have that $\sigma \in \overline{H}$ iff for all $\lambda \in \Lambda$, $\sigma N_\lambda \cap H \neq \varnothing$. Now, if $\sigma N_\lambda \cap H$, then we have that there is an $n_\lambda \in N_\lambda$ so that $\sigma n_\lambda = h_\lambda \in H$; i.e., $\sigma = h_\lambda n_\lambda^{-1}$. But if $\sigma = h_\lambda n_\lambda^{-1}$, then this implies that $\sigma \in H N_\lambda^{-1} = H N_\lambda$. This is true for all λ, so combining these all together, we have

$$\sigma \in \overline{H} \iff \sigma \in \bigcap_\lambda H N_\lambda.$$

Hence, $\overline{H} = \bigcap_\lambda H N_\lambda$. □

We now have the ingredients to prove the proposition.

Proof of proposition. ($\implies$) Assuming that H is a closed subgroup of G, we get that $H = \overline{H} = \bigcap_\lambda HN_\lambda$. Notice that $HN_\lambda = \bigcup_{h\in H} hN_\lambda$, hence each HN_λ is open. Since N_λ is a normal subgroup, HN_λ is a subgroup of G, so HN_λ is an open subgroup of G. Hence, take $U_\lambda = HN_\lambda$ and $A = \Lambda$.
($\impliedby$): If $H = \bigcap_\alpha U_\alpha$, then since each U_α is an open subgroup, U_α is also a closed subgroup, finishing the proof. □

A consequence of this is the following.

Corollary 28. Let $F \subset K \subset E$ be any intermediate field. Then $\mathrm{Gal}(E/K)$ is closed in $\mathrm{Gal}(E/F)$.

Proof. This follows by the observation that

$$\mathrm{Gal}(E/K) = \bigcap_{\alpha\in K} \mathrm{Gal}(E/F(\alpha))$$

and the fact that $(F(\alpha) : F) < \infty$. The first proposition gives us that these are open, and the second proposition tells us that $\mathrm{Gal}(E/K)$ is closed. □

TODO: FINISH WEEK14 NOTES

References

[1] Nathan Jacobson. *Basica Algebra II*. Second Edition.
[2] Emil Artin. *Galois Theory*. Notre Dame Mathematical Lectures No. 2.
[3] James Cogdell. *Lecture Notes*. Spring 2020.
[4] James Milne. *Fields and Galois Theory*. Version 4.61. Link
[5] Serge Lang. *Algebra*. Revised Third Edition.
[6] David McReynolds. *Galois Theory*. Spring 2017. Link