§ Lecture 1

Definition 1.1. Let F be a field. A *field extension* of F is a field E with a ring homomorphism $i : F \to E$.

This homomorphism is automatically injective, so it identifies F with a subfield of E. Let $F[X]$ denote the ring of polynomials with coefficients in F. Since F is a field, $F[X]$ is a principle ideal domain. This means that any ideal of $F[X]$ is generated by a single polynomial f, and in particular, it is prime if and only if f is irreducible. Since prime ideals are maximal in a principal ideal domain, we get the following:

Theorem 1.1. *Let F be a field. Then $F[X]/(f)$ is a field if and only if f is irreducible.*

Consider the composition of maps $F \hookrightarrow F[X] \to F[X]/(f)$. This defines a ring homomorphism from F to $F[X]/(f)$, and so $F[X]/(f)$ is a field extension of F. Moreover, in this extension f has a root, namely the coset of X in the quotient ring. This proves the following lemma:

Lemma 1.2. *Let f be any polynomial in $F[X]$. Then there exists a field extension of F where f has a root.*

Now consider a field extension E/F, and let α be an element of E. Then we can think about the evaluation map $\phi_\alpha : F[X] \to E$ mapping each polynomial $f \in F[X]$ to $f(\alpha)$. If $\ker \phi_\alpha = 0$, then there is no non-zero polynomial $f \in F[X]$ which has α as a root, and also the map is injective. We say that α is transcendental over F in this case. Otherwise, $\ker \phi_\alpha$ is generated by a polynomial f, which we can assume to be monic. By the first isomorphism theorem, we have

$$\frac{F[X]}{(f)} = \frac{F[X]}{\ker \phi_\alpha} \cong \operatorname{Im} \phi_\alpha \subset E.$$

Therefore, $\operatorname{Im} \phi_\alpha$ is an integral domain and hence f is an irreducible polynomial. It is called the minimal polynomial of α over F, and we say that α is algebraic over F in this case. We then define $\deg \alpha = \deg f$ as a polynomial. It is easy to see that any polynomial $g \in F[X]$ also satisfying $g(\alpha) = 0$ must be divisible by f in $F[X]$.

Let $F(\alpha)$ be the smallest subfield of E containing both F and α. Then we have the following theorem.

Theorem 1.3. *Let E/F be a field extension and $\alpha \in E$. Let $\phi_\alpha : F[X] \to E$ be the evaluation map. Then*

1. *If α is transcendental over F, then $F(\alpha) \cong F(X)$, the field of rational functions with coefficients in F.*
2. *If α is algebraic, then $F(\alpha) = \operatorname{Im} \phi_\alpha \cong F[X]/(f)$.*

Proof. If α is transcendental, then ϕ_α is injective, so $F[X] \cong \operatorname{Im} \phi_\alpha$, and consequently $F(X) = \operatorname{Frac}(F[X]) \cong \operatorname{Frac}(\operatorname{Im} \phi_\alpha)$. Since any field containing F and α must also contain $\operatorname{Im} \phi_\alpha$ and hence also $\operatorname{Frac}(\operatorname{Im} \phi_\alpha)$, we see that $F(X) \cong \operatorname{Frac}(\operatorname{Im} \phi_\alpha) = F(\alpha)$.

If α is algebraic with minimal polynomial f, then by the same reasoning as above we have $\operatorname{Frac}(F[X]/(f)) \cong \operatorname{Frac}(\operatorname{Im} \phi_\alpha) = F(\alpha)$. However, $F[X]/(f) \cong \operatorname{Im} \phi_\alpha$ is already a field, and the desired isomorphism follows. □

We say that a field extension E/F is simple if it is generated by a single element, i.e. $E = F(\alpha)$ for some $\alpha \in E$. (It turns out that a lot of the extensions that we are interested in are simple by the primitive element theorem.)

Theorem 1.4. *Let $E = F(\alpha)$ be a field extension of F where α is algebraic with* $\deg \alpha = n$. *Then E is an n-dimensional vector space over F with basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.*

Proof. Trivial. □

§ Lecture 2

First, let's define what a vector space is.

Definition 2.1. A *vector space* over a field F is an abelian group V with the scalar multiplication map $\cdot : F \times V \to V$ satisfying the usual axioms.

Example 2.1.1. If E/F is a field extension, then E is a vector space over F.

Define linear independence, span, bases, etc. as usual.

Question. Suppose that V is the vector space of convergent power series over $\mathbb{R}$. Does V have a countable spanning set?

Solution by Hein. The answer is no. Consider the family $\{e^{\alpha x}\}_{\alpha \in \mathbb{R}}$. The vectors in this family are linearly independent (which can be shown by differentiation). Therefore, for any spanning set S of V, we must have $|S| > |\mathbb{R}|$, so there is no countable spanning set. □

§ Lecture 3

Definition 3.1 (algebraic extension)**.** Let E/F be a field extension. E is an algebraic extension over F if every element $\alpha \in E$ is algebraic over F.

Example 3.1.1. $\mathbb{C}/\mathbb{R}$ is algebraic. Let $z \in \mathbb{C}$. Then $f(x) = (x - z)(x - \overline{z}) \in \mathbb{R}[x]$ has z as a root.

Question. What is the biggest algebraic extension of $\mathbb{Q}$ inside $\mathbb{R}$?

Here is a different, stronger 'finiteness' condition on field extensions.

Definition 3.2 (finite extension)**.** E/F is a finite extension if it is a finite dimensional vector space over F.

Example 3.2.1. Let E/F be an arbitary field extension, and let $\alpha \in E$ be algebraic over F. Then $F(\alpha)/F$ is a finite field extension with degree $\deg \alpha$.

Finite extensions are a subset of algebraic extensions.

Theorem 3.1. *If E/F is finite then it is algebraic.*

Proof. Let E/F be finite of degree n, and let $\alpha \in E$. Consider $1, \alpha, \alpha^2, \ldots, \alpha^n$. These elements must be linearly dependent over F (since there are $n+1$ of them), so there exists some $c_0, c_1, \ldots, c_n \in F$, not all zero, such that

$$c_n \alpha^n + c_{n-1} \alpha^{n-1} + \cdots + c_0 = 0.$$

Hence α is algebraic over F. □

However, not all algebraic extensions are finite! We are not ready to prove this yet, but we can try to convince ourselves that this is true. Consider $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[5]{2}, \sqrt[7]{2}, \ldots)$. This is *probably* not finite but it is definitely algebraic.

Definition 3.3. Let E/F be finite. Then the dimension of E as a vector space over F is denoted as $[E : F] = \dim_F E$.

Theorem 3.2. *Let E/F and K/E be field extensions. Then K is also an extension of F. Suppose that K/F is finite. Then E/F and K/E are also finite, and*

$$[K : F] = [K : E][E : F].$$

Proof. Since a subspace of a finite dimensional vector space is also finite dimensional, it follows that $[E : F]$ is finite. Moreover, if a set of vectors $S \subset K$ is linearly independent over E, then they must also be linearly independent over F, so it follows that $[K : E]$ is finite as well. Let $e_1, \cdots, e_m$ be a basis of E over F and let $k_1, \cdots, k_n$ be a basis of K over E. Let α be an element of E. Then α can be written as a linear combination of k_i with coefficients from E, each of which can be written as linear combinations of e_i with coefficients from F. This shows that α can be written as a linear combination of $e_i k_j$ over F. It is also easy to see that they are linearly independent over F, so it follows that they form a basis of K over F and that $[K : F] = mn = [K : E][E : F]$. □

The usage of this theorem is similar to Lagrange's theorem in group theory. In particular, we have the following corollary.

Corollary 3.2.1. *Let $\alpha \in E/F$ be algebraic over F. Let $\beta \in F(\alpha)$. Then* $\deg \beta$ *divides* $\deg \alpha$.

Finite extensions are finitely generated.

Theorem 3.3. *Let E/F be finite. Then there exist $\alpha_1, \ldots, \alpha_n \in E$ such that $E = F(\alpha_1, \ldots, \alpha_n)$.*

Proof. We can just take $\alpha_1, \ldots, \alpha_n$ to be a basis of E over F. □

The converse of the above theorem holds as well.

Theorem 3.3 (Converse). *If $\alpha_1, \ldots, \alpha_n$ are algebraic over F, then $F(\alpha_1, \ldots, \alpha_n)$ is finite.*

Proof. Note that $\deg(\alpha_i, F(\alpha_1, \ldots, \alpha_{i-1})) \leq \deg(\alpha_i, F)$. Therefore, it is finite. Now we can rewrite the degree we want as

$$[F(\alpha_1, \ldots, \alpha_n) : F] = [F(\alpha_1) : F][F(\alpha_1, \alpha_2) : F(\alpha_1)] \cdot \ldots \cdot [F(\alpha_1, \ldots, \alpha_n) : F(\alpha_1, \ldots, \alpha_{n-1})].$$

Therefore, we are done by Theorem 3.2. □

Definition 3.4. Let E/F be an extension. The algebraic closure of F in E, denoted $\overline{F}_E$, is the set of $\alpha \in E$ which are algebraic over F.

The set of algebraic elements forms a field.

Theorem 3.4. *$\overline{F}_E$ is a subfield of E.*

Proof. Suppose that $\alpha, \beta \in E$ are algebraic over F. Then $F(\alpha, \beta)$ has finite degree, hence algebraic. Since $\alpha + \beta, \alpha\beta, -\alpha, \alpha^{-1}$ all belong to $F(\alpha, \beta)$, it follows that they are all algebraic. Hence $\overline{F}_E$ is a subfield of E. □

Definition 3.5. F is algebraically closed if every non-constant polynomial $f \in F[X]$ has a root in F.

Theorem 3.5 (Fundamental Theorem of Algebra). *$\mathbb{C}$ is algebraically closed.*

Proof. Let $f(z)$ be a polynomial with coefficients in $\mathbb{C}$. Suppose f has no roots in $\mathbb{C}$. Consider $1/f(z)$. This is a bounded entire function on $\mathbb{C}$, so by Liouville's theorem it follows that $1/f(z)$ is constant. Hence f is a constant polynomial. □

Our definition of an algebraically closed field is a lot stronger than it looks.

Theorem 3.6. *F is algebraically closed iff every nonconstant polynomial $f \in F[X]$ splits as a product of linear factors:*

$$f = \alpha_0(x - \alpha_1) \cdots (x - \alpha_n), \qquad \alpha_i \in F.$$

Proof. Factor theorem and induction. □

Theorem 3.7. *F is algebraically closed iff there are no non-trivial algebraic extensions of F.*

Proof. Let F be algebraically closed and let E/F be algebraic. Let $\alpha \in E$. Consider the irreducible polynomial $f \in F[X]$ which has α as one of its roots. Since F is algebraically closed, it follows that

$$f(\alpha) = (\alpha - \alpha_1)(\alpha - \alpha_2) \cdots (\alpha - \alpha_n) = 0. \qquad \alpha_i \in F.$$

Therefore, $\alpha = \alpha_i$ for some i and hence $\alpha \in F$. □

§ Lecture 4

Definition 4.1. Let F be a field. An *algebraic closure* of F is a field extension E such that E/F is algebraic and E is algebraically closed.

Example 4.1.1. $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$.

Example 4.1.2. Let $\overline{\mathbb{Q}} \subset \mathbb{C}$ be the set of elements of $\mathbb{C}$ algebraic over $\mathbb{Q}$. Then $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$.

Example 4.1.3. Let $F = \mathbb{C}((z))$ be the field of complex Laurent series (power series where we allow a finite number of negative terms.) Then an algebraic closure $\overline{F}$ is given by the field of Puiseux series:

$$\overline{F} = \left\{ \sum_{k=n}^{\infty} a_k z^{\frac{k}{\ell}} \,\middle|\, n \in \mathbb{Z}, \ell \in \mathbb{Z}^+, a_k \in \mathbb{C} \right\}.$$

Question. Show that F is actually a field.

Note that by Lemma 1.2, given a field F and a polynomial f, there exists a field extension E/F such that f splits completely as linear factors in $E[X]$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of f in E.

Definition 4.2. The field $F(\alpha_1, \ldots, \alpha_n)$ is called a splitting field of f.

Splitting fields are unique up to isomorphism. They can be thought of as a miniature version of the construction of algebraic closures, since in the latter we went every polynomial to split, not just a single one.

Lemma 4.1. *Suppose that F/k and E/F are algebraic field extensions. Then E/k is also algebraic.*

Proof. Take any element $\alpha \in E$. Since α is algebraic over F, there exist $a_0, \ldots, a_n \in F$ such that

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

Now consider the chain of field extensions $k \subseteq k(a_0, \ldots, a_n) \subseteq k(a_0, \ldots, a_n, \alpha)$. Each a_i is algebraic over k since F is algebraic over k. Therefore, $k(a_0, \ldots, a_n)/k$ is finite by Theorem 3.3. Moreover, $k(a_0, \ldots, a_n, \alpha)/k(a_0, \ldots, a_n)$ is finite since we are adjoining a single algebraic element. Since a chain of finite field extensions is also finite, we see that $k(a_0, \ldots, a_n, \alpha)/k$ is also finite, hence algebraic. In particular, α is algebraic over k as desired. □

Theorem 4.2. *Let F be a field. Then there exists an algebraic closure of F, which is denoted as $\overline{F}$.*

Proof. First, let's assume that F is countable. Then the set of degree d polynomials in $F[X]$ is countable for each $d \geq 1$ and consequently their union $F[X]$ is also countable. Make a list of all polynomials, say $p_1, p_2, \ldots$. We can now repeatedly use the construction of splitting fields to create a very large field where every p_i splits. To be more precise, let F_1/F be the splitting field of p_1 over F, and in general, let F_i/F_{i-1} be the splitting field of p_i over F_{i-1}. Then define $\overline{F} = \bigcup_{n\geq 1} F_n$.

Obviously, $\overline{F}$ contains all the roots of polynomials in $F[X]$. Moreover, $\overline{F}$ is algebraic over F, since any element in it must be contained in F_n for some $n \geq 1$ and F_n/F is algebraic by Lemma 4.1 (This also follows from the fact that the construction of F_n is done entirely by adjoining algebraic elements over F.) We now claim that $\overline{F}$ is algebraically closed. Take any polynomial $f \in \overline{F}[X]$, and let $E/\overline{F}$ be a splitting field of f over F. Let α be any root of f in E. Then both the field extensions $\overline{F}/F$ and $\overline{F}(\alpha)/\overline{F}$ are algebraic, so it follows that $\overline{F}(\alpha)/F$ is also algebraic. Hence α is a root of a polynomial in $F[X]$, and consequently, $\alpha \in \overline{F}$. This shows that $\overline{F}$ is algebraically closed as desired.

Now suppose that F is uncountable. Then consider the partially-ordered set of algebraic extensions of F. Every chain has an upper bound since we can just take the union, so by Zorn's lemma there exists a maximal element. It is then easy to show that this maximal element is algebraically closed by the same logic as above. □

§ Lecture 5

Definition 5.1. A *straightedge* is an infinitely long ruler without any markings on it. A *compass* is just like a regular one.

In Euclid's original formulation, the compass collapses on itself once it is lifted from the paper so you cannot transfer lengths just by using it. However, it can be shown that this formulation is in fact no weaker than ours.

Definition 5.2. A real number $\alpha \in \mathbb{R}$ is constructible if a segment of length $|\alpha|$ can be constructed from a length 1 segment using a ruler and a compass.

Question (Important!)**.** Can we characterize the set of all constructible numbers in $\mathbb{R}$?

Theorem 5.1. *The set of constructible numbers forms a subfield of real numbers.*

We can even take square roots! This follows from the construction of geometry mean of two numbers. But this is all we can do, as claimed by the following theorem.

Theorem 5.2. *All constructible numbers are obtained from 1 by the 5 operations $+, -, \times, \div, \sqrt{}$.*

Sketch. Suppose that we have some constructible points $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{R}^2$, and we can use those to contruct a point β by just one step. By solving the equations in cartesian coordinates, we can show that the coordinates of β are obtained from those of $\alpha_1, \alpha_2, \ldots, \alpha_n$ by the 5 operations as mentioned above. Therefore, by induction, we can show that every constructible number is obtained from 1 using the 5 operations. □

Now we are ready to nuke the classic problems using field theory.

Theorem 5.3. *It is impossible to double the cube.*

Proof. It is enough to show that $\sqrt[3]{2}$ is not a constructible number. Note that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. However, if α is obtained from a sequence of square roots, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^d$ for some d. Hence if $\alpha \in \mathbb{Q}(\sqrt[3]{2})$ and α is constructible, then $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divides $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$, so $\alpha \in \mathbb{Q}$. In particular, this shows that $\sqrt[3]{2}$ is not constructible. □

§ Lecture 6

Definition 6.1. Given an integral domain R, the *characterisitic* of R is the smallest integer $n \in \mathbb{Z}_{>0}$ such that $nr = 0$ for all $r \in \mathbb{R}$.

Lemma 6.1. *The characterisitic of an integeral domain is either a prime number or ∞.*

Theorem 6.2. *Let $\mathbb{F}$ be a field with characteristic p. Then $\mathbb{F}$ is an extension of $\mathbb{F}_p$. In particular, if $\mathbb{F}$ is finite, then $\mathbb{F}$ has p^n elements.*

From now on we will let $\mathbb{F}$ to be a finite field of characteristic p. Our goal is to show that $\mathbb{F} = \mathbb{F}_p(\alpha)$ for some $\alpha \in \mathbb{F}_p$, in other words, the extension $\mathbb{F}/\mathbb{F}_p$ is simple. Let $\mathbb{F}^\times \subset \mathbb{F}$ be the unit group of $\mathbb{F}$. Then in fact we have the following:

Theorem 6.3. *$\mathbb{F}^\times$ is a cyclic group!*

Proof. $\mathbb{F}^\times$ is a finite abelian group, so by the classification theorem,

$$\mathbb{F}^\times = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k},$$

where each d_i is a prime power. In particular, $\mathbb{F}^\times$ is cyclic if all the primes occuring are distinct.

Let m be the least common multiple of all d_i. Then every element of $\mathbb{F}^\times$ has order dividing m. Therefore, every element of $\mathbb{F}$ is a root of the polynomial $X^{m+1} - X \in \mathbb{F}[X]$. Hence, $m \geq |\mathbb{F}^\times|$. On the other hand, $m \leq d_1 \cdot \ldots \cdot d_k = |\mathbb{F}^\times|$. Therefore, $m = |\mathbb{F}^\times|$, and hence all the prime powers are distinct. In particular, $\mathbb{F}^\times$ is cyclic by the chinese remainder theorem. □

Now we have our desired result as a corollary.

Corollary 6.3.1. *$\mathbb{F}/\mathbb{F}_p$ is a simple extension.*

Our next goal is to show the existence of finite fields of size p^n for any prime p and any integer $n > 0$. This is easy to show using the following theorem.

Theorem 6.4. *Let $\mathbb{F}$ be a field of size p^n. Then every $\alpha \in \mathbb{F}$ is a root of $X^{p^n} - X$.*

Therefore, $\mathbb{F}$ can be obtained by adjoining roots of $X^{p^n} - X$ over $\mathbb{F}_p$. This is formalized in the following theorem:

Theorem 6.5. *Let $\overline{\mathbb{F}_p}$ be an algebraic closure of $\mathbb{F}_p$, and let E denote the set of roots of $X^{p^n} - X$ in $\overline{\mathbb{F}_p}$. Then E is a finite field of order p^n.*

§ Lecture 7

We will divide the proof of Theorem 6.5 to two parts. The proof that E is a field is quite easy so we just need to show the following lemma.

Lemma 7.1. *$X^{p^n} - X$ has p^n distinct roots in $\overline{\mathbb{F}_p}$.*

Proof. Suppose that α is a root of $f(X) = X^{p^n} - X$. Then

$$\frac{f(X)}{X-\alpha} = \frac{1}{X-\alpha}(X^{p^n} - \alpha^{p^n} - X + \alpha) = X^{p^n-1} + X^{p^n-2}\alpha + \cdots + X\alpha^{p^n-2} + \alpha^{p^n-1} - 1.$$

Evaluating this polynomial at $X = \alpha$ gives

$$\alpha^{p^n-1} + \alpha^{p^n-1} + \cdots + \alpha^{p^n-1} - 1 = p^n(\alpha^{p^n-1}) - 1 = -1 \neq 0.$$

Therefore, α is not a double root of f and we're done. □

Since $\mathbb{F}_q$ is a simple extension of degree n over $\mathbb{F}_p$, it follows that there exists an irreducible polynomial $f \in \mathbb{F}_p[X]$ of degree n such that $\mathbb{F}_q \cong \mathbb{F}_p[X]/(f)$. Moreover, f divides $X^{p^n} - X$ since all its roots are the roots of $X^{p^n} - X$.

Finite fields are essentially unique.

Theorem 7.2. *Let E, E' be two finite fields of size p^n. Then $E \cong E'$.*

Proof. Let $E = \mathbb{F}_p(\alpha)$. Then α is a root of an irreducible polynomial $f(X) \in \mathbb{F}_p[X]$, and $f(X) \mid X^{p^n} - X$. E' also contains the roots of $X^{p^n} - X$, so in particular it contains all the roots of f. Let β be such a root. Then we can construct an isomorphism $\mathbb{F}_p(\alpha) \cong \mathbb{F}_p(\beta) \subset E'$. Since all the fields are finite and have the same size it follows that $\mathbb{F}_p(\beta) = E'$. □

§ Lecture 8

Definition 8.1. Let E/F be an extension. Let $\alpha, \beta \in E$. Then α and β are *conjugate* if they satisfy the same irreducible polynomial over F.

Example 8.1.1. Let z be a complex number not in $\mathbb{R}$. Then z and $\overline{z}$ are conjugates since they are both roots of the irreducible polynomial $f(x) = (x-z)(x-\overline{z}) = x^2 - (z+\overline{z})x + z\overline{z} \in \mathbb{R}[x]$.

Conjugates are basically 'indistinguishable' from each other.

Theorem 8.1. *Let $F(\alpha)$ be a simple extension of F. Let $F(\beta)$ be another simple extension. Then there exists an isomorphism $\tau : F(\alpha) \to F(\beta)$ which fixes F and takes α to β iff α and β are conjugates.*

Proof. Suppose that there exists such a map τ, and let f be the minimal polynomial of α over F. Then since τ fixes the elements of F,

$$0 = \tau(f(\alpha)) = f(\tau(\alpha)) = f(\beta),$$

so β is also a root of f, and hence α and β are conjugate to each other. On the other hand, if α and β are roots of the same irreducible polynomial f, then we can construct an isomorphism

$$F(\alpha) \cong \frac{F[X]}{(f)} \cong F(\beta).$$

This isomorphism fixes F. Moreover, α is send to the coset of X which is sent to β so we are done. □

Example 8.1.2. Consider $\mathbb{Q}(i)$ and $\mathbb{Q}(-i)$. Then since i and $-i$ are conjugate, we have an isomorphism $\mathbb{Q}(i) \to \mathbb{Q}(-i)$ which fixes $\mathbb{Q}$ and sends i to $-i$. In other words, this is just the complex conjugation map $z \to \overline{z}$.

Corollary 8.1.1. *Let $F(\alpha)$ be a simple extension. Let $\overline{F}$ be an algebraic closure of F. Then the embeddings $F(\alpha) \to \overline{F}$ fixing F are indexed by the conjugates of α in $\overline{F}$. In particular, there are* $\deg \alpha$ *such embeddings.*

Example 8.1.3. There are two embeddings of $\mathbb{Q}(i)$ in $\overline{\mathbb{Q}}$ which fixes $\mathbb{Q}$: the identity map, and the conjugation map.

Definition 8.2. Let F be a field. An *automorphism* of F is an isomorphism from F to itself.

§ Lecture 9

Definition 9.1. Let E be a field extension of F. We define $G(E/F)$ be the set of automorphisms $\tau : E \to E$ which fix F. G forms a group under function composition.

Let's take a look at a couple of examples of automorphism groups.

Example 9.1.1. There are only two automorphisms of $\mathbb{C}$ fixing $\mathbb{R}$, namely identity and conjugation. Therefore, $G(E/F) \cong \mathbb{Z}/2\mathbb{Z}$.

Example 9.1.2. Note that $\sqrt{2}$ and $-\sqrt{2}$ are conjugate over $\mathbb{Q}$. Therefore, the only automorphisms of $\mathbb{Q}(\sqrt{2})$ fixing $\mathbb{Q}$ are the identity map and the map $a + b\sqrt{2} \to a - b\sqrt{2}$. Again, we have $G(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

Example 9.1.3. Consider $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. The only conjugate of $\sqrt[3]{2}$ inside $\mathbb{Q}(\sqrt[3]{2})$ is itself, so it follows that $G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is the trivial group.

Example 9.1.4. Consider $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. Then there are two automorphisms of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and two of $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$. Then, some computations show that $G(\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Example 9.1.5. Consider $\mathbb{F}_{p^2}/\mathbb{F}_p$. This is generated by an element α which has multiplicative order $p^2 - 1$ and degree 2. Now consider the map $\phi : \mathbb{F}_{p^2} \to \mathbb{F}_{p^2}$ given by $a \to a^p$. It is easy to check that this is a field homomorphism, so injective, and since the fields are finite, it is also surjective. Therefore, ϕ is an isomorphism, and ϕ is identity on $\mathbb{F}_p$ by Fermat's little theorem, so $\phi \in G(\mathbb{F}_{p^2}/\mathbb{F}_p)$.

The following theorem is not as strong as it looks!

Theorem 9.1. *Let $F(\alpha)/F$ be a simple extension. Let $\alpha_1, \alpha_2, \ldots, \alpha_k$ be the conjugates of α in $F(\alpha)$. Then $G(F(\alpha)/F)$ is a subgroup of the symmetric group S_k.*

Proof. An automorphism τ is fully determined by the image of α under τ, which belongs to the set $C = \{\alpha_1, \ldots, \alpha_k\}$. Moreover, $\tau(\alpha_i) = \alpha_j$ for all $1 \leq i \leq k$. Therefore, τ permute the elements of C in a unique way, so we can construct a injective homomorphism from $G(F(\alpha)/F) \to S_k$. □

Example 9.1.6 (Cyclotomic Extensions)**.** Consider the polynomial $\frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + 1 \in \mathbb{Q}[x]$ where p is a prime. This polynomial is irreducible by Eisenstein's criterion, so we can construct a field extension $\mathbb{Q}[x]/(f) \cong \mathbb{Q}(\zeta_p)$, where ζ_p is a pth root of unity and $\zeta_p \neq 1$. Then the automorphism group consists of automorphisms τ_k which map ζ_p to ζ_p^k. Therefore, $G(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

§ Lecture 10

Suppose that we have a field isomorphism $\tau : F \to F'$. Consider an algebraic closure of F', say $\overline{F'}$, and consider an algebraic extension E/F. Can we extend τ to a map from E into $\overline{F}$? As you would expect, the answer is yes!

Theorem 10.1. *τ can be extended to a map $\sigma : E \to \overline{F'}$, such that $\sigma(r) = \tau(r)$ for $r \in F$.*

Proof. Consider the set $S = \{(E', \tau')\}$, where E' is an intermediate field between F and E, and τ' is an extension of τ. This set is non-empty and partially ordered by the relation $\leq$, where we say that $(E_1, \tau_1) \leq (E_2, \tau_2)$ if E_1 is a subfield of E_2 and τ_2 is an extension of τ_1. It is easy to check that any chain has an upper bound by taking unions, so by Zorn's lemma there exists a maximal element (E_0, τ_0). We claim that $E_0 = E$. Let the image of E_0 under τ_0 be $L \subset \overline{F'}$. If $E_0 \neq E$, then there exists an element $\alpha \in E$ not contained in E_0. Let f be the minimal polynomial of α over E_0. Then we have the isomorphisms

$$E_0(\alpha) \cong \frac{E_0[X]}{(f)} \cong \frac{L[X]}{(\tau_0(f))} \cong L(\alpha_0) \subseteq \overline{F'},$$

where α_0 is a root of $\tau_0(f)$ in $\overline{L'}$. This contradicts the maximality of (E_0, τ_0), so it follows that $E_0 = E$. □

Here is a nice corollary.

Corollary 10.1.1. *Let F be a field. Then any two algebraic closures of F are isomorphic.*

Proof. Let $\overline{F_1}$ and $\overline{F_2}$ be two algebraic closures of F. Then we have inclusion maps τ_1 and τ_2 from F to each of them. By our theorem, we can extend τ_2 to a map $\overline{\tau} : \overline{F_1} \to \overline{F_2}$. Consider the image $\overline{\tau}(\overline{F_1}) = L \subset \overline{F_2}$. We then have $\overline{\tau}^{-1} : L \to \overline{F_1}$. We can again extend this to a field homomorphism $\chi : \overline{F_2} \to \overline{F_1}$. Then χ is an isomorphism when restricted to $\overline{F_2}$ and since χ is injective, we can conclude that $L = \overline{F_2}$. □

§ Lecture 11

Theorem 11.1. *Let E/F be a finite extension. Then the group of automorphisms $G(E/F)$ is also finite.*

Proof. Let $S \coloneqq \{\alpha_1, \ldots, \alpha_n\}$ be the set of generators of E over F. Then the possible images of α_i under ϕ is finite for each i. Since ϕ is completely determined by the image of α_i, it follows that $G(E/F)$ is also finite. □

Definition 11.1. For a field extension E/F, the index of E/F, which we denote by $\{E : F\}$ is the number of field homomorphisms from F to an algebraic closure of F.

Of course, we first have to show that this value does not depend on the algebraic closure chosen.

Theorem 11.2. *Let $\overline{F}$ and $\overline{F}'$ be two algebraic closures of F. Then $\{E : F\}_{\overline{F}} = \{E : F\}_{\overline{F}'}$.*

Proof. We have an isomorphism $\tau : \overline{F} \to \overline{F}'$ which extends the identity on F. Then any homomorphism from E to $\overline{F'}$ which fixes F can be composed with τ to get a homomorphism from E to $\overline{F}'$ which fixes F and vice versa. □

Therefore, from now on we will just drop the subscript. Also, we can easily extend this to isomorphisms other than the identity.

Corollary 11.2.1. *Suppose that $\sigma : F \to F'$ is an isomorphism. Then the number of homomorphisms from E to $\overline{F'}$ which extend σ is equal to $\{E : F\}$.*

The index is multiplicative as you might expect from the name.

Lemma 11.3. *Suppose that $E \subseteq F \subseteq K$ is a tower of finite extensions. Then*

$$\{K : E\} = \{K : F\}\{F : E\}.$$

Proof. Fix an algebraic closure of E, say $\overline{E}$, and take any homomorphism τ from $F \to \overline{E}$ which fixes E. Then take a homomorphism σ from $K \to \overline{E}$ extending $\tau : F \to \tau(F) \subset \overline{E}$. Then σ is a homomorphism from $K \to \overline{E}$ which fixes E. There are $\{F : E\}$ choices of τ, and for each choice of τ, there are $\{K : F\}$ choices for σ. Therefore,

$$\{K : E\} = \{K : F\}\{F : E\}$$

as desired. □

Now let's actually talk about splitting fields!

Definition 11.2. Given a set of $\{f_i\}_{i\in I} \subseteq F[X]$, the *splitting field* of $\{f_i\}_{i\in I}$ over F is defined to be the smallest subfield of $\overline{F}$ containing the roots of $f_i(x)$ for every $i \in I$.

In particular, if the set of polynomials is finite, say $I = \{f_1, \ldots, f_n\}$, then the splitting field of I over F is the same as the splitting field of $f_1 \cdot \ldots \cdot f_n$ over F.

As a silly reminder, we will say that a field is a splitting field over F if it is a splitting field of some $I \subset F[x]$.

Example 11.2.1. The field $\mathbb{Q}(\sqrt[3]{2})$ is not a splitting field over $\mathbb{Q}$! This is not as obvious as it looks since it can be the splitting field of some polynomial other than $X^3 - 2$.

§ Lecture 12

It turns out that there are a lot of nice characterizations of splitting fields. Here is one of them.

Theorem 12.1. *Let $F \subseteq K \subseteq \overline{F}$ be a tower of field extensions. Then the following are equivalent.*

1. *K is a splitting field.*
2. *For any automorphism $\sigma \in G(\overline{F}/F)$, $\sigma|_K$ is an automorphism of K.*

Proof. Let's first show that (1) implies (2). Suppose that K is a splitting field over F of a set of polynomials $I \subseteq F[X]$. Let S be the set of all the roots of polynomials in I. Then we claim that $F[S] = K$. Take any non-zero element α of $F[S]$. Then α is algebraic over F, so there exists an irreducible polynomial $f \in F[X]$, such that $f(\alpha) = 0$. But this means that we can express α^{-1} as a linear combination of sums of powers of α with coefficients in F. Therefore, $\alpha^{-1} \in F[S]$, and consequently, $F[S]$ is a field. Therefore, by the minimality of the splitting field, we must have $F[S] = K$. Moreover, σ permutes the elements of S, since it sends each element to its conjugate. Therefore, σ is an automorphism on $F[S] = K$ as desired.

Now let's show that (2) implies (1). Take any element $\alpha \in K$, and let $\overline{\alpha}$ be any of its conjugates over F. Then there exists an isomorphism $\tau : F(\alpha) \to F(\overline{\alpha})$, and by the properties of algebraic closures, we can extend this to a field automorphism $\overline{\tau} : \overline{F} \to \overline{F}$. Then $\overline{\tau}(K) = K$, so $\overline{\alpha} \in K$. Now let $\{f_i\}_{i\in I}$ be the set of polynomials which has a root in K. Then it immediately follows that K is the splitting field of $\{f_i\}_{i\in I}$. □

§ Lecture 13

From above, we get this amazing result as a corollary.

Corollary 13.0.1. *Any irreducible polynomial $f \in F[X]$ which has at least one root in K has all roots in K.*

Proof. Let α be a root of f, and let β be any of its conjugates in $\overline{F}$. Then there exists an automorphism $\sigma : F(\alpha) \to F(\beta)$ which sends α to β, and this can be extended to a homomorphism $\overline{\sigma} : \overline{F} \to \overline{F}$. However, by the above theorem, $\overline{\sigma}$ sends K to K, so $\beta = \overline{\sigma}(\alpha) \in K$. Therefore, all conjugates of $\alpha \in \overline{F}$ actually belong to K, and so f splits completely in K. □

It is also easy to show that the following holds:

Corollary 13.0.2. *If K/F is a splitting field of finite degree, then $\{K : F\} = |G(K/F)|$.*

Now let's talk about separable extensions.

Definition 13.1. Given $f \in F[X]$ and α a root of f, then the multiplicity of α is the largest naturnal number n such that $(x - \alpha)^n$ divides f in its splitting field.

If f is irreducible, then it is reasonable to expect that all roots of f have multiplicity 1. However, this is not necessarily true for every field!

Example 13.1.1. Consider $F = \mathbb{F}_p(t)$. Then the polynomial $f = X^p - t \in F[X]$ is irreducible by Eisenstein's criterion and Gauss' lemma. However, if s is a root of f in an extension field of F, then $(X - s)^p = X^p - s^p = X^p - t$. Therefore, s has multiplicity p.

Instead, we can show the following weaker, but still quite interesting result.

Theorem 13.1. *Let $f \in F[X]$ be an irreducible polynomial. Then all roots of f have the same multiplicity.*

Proof. Let α be a root of f in K with multiplicity n. Let β be any other root of f in K. Then we can construct an automorphism $\sigma : F(\alpha) \to F(\beta)$. This induces an automorphism $\tau : F(\alpha)[X] \to F(\beta)[X]$. Then $\tau(X - \alpha) = X - \beta$ but $\tau(f) = f$ since $f \in F[X]$. Therefore, β has the same multiplicity as α. □

Lemma 13.2. *Let $f(x) \in F[X]$ and α be a root of f. Then $\{F(\alpha) : F\}$ is the number of distinct roots of f in its splitting field.*

Proof. This follows since two homomorphisms σ and τ from $F(\alpha)$ to $\overline{F}$ which fix F are identical if and only if $\sigma(\alpha) = \tau(\alpha)$, and any homomorphism τ must send α to a root of f inside $\overline{F}$. □

Theorem 13.3. *Let E/F be a finite extension, then*

$$\{E : F\} \mid [E : F].$$

Proof. It suffices to show this for simple extensions since both quantities are multiplicative. Let α be an element of $\overline{F}$ and let f be the minimal polynomial of α over F. By the above lemma, $\{F(\alpha) : F\}$ is the number of distinct roots of f, where $[F(\alpha) : F]$ is the total number of roots of f. Since all roots of f have the same multiplicity, say n, it follows that $\{F(\alpha) : F\} = n[F(\alpha) : F]$. □

There are many different definitions of separable extensions. Here is one of them:

Definition 13.2. We say that a polynomial $f \in F[X]$ is separable if all its roots have multiplicity 1 in its splitting field. A field extension E/F is separable if the irreducible polynomial of α over F is separable for all $\alpha \in E$.

The separability of a polynomial thus do not depend on the field in which it splits into linear factors, since all such fields contain an isomorphic copy of the splitting field of the polynomial. Therefore, we can talk about whether a polynomial is separable or not without reference to the field in which it splits.

Lemma 13.4. *Consider the tower of finite field extensions $F \subseteq E \subseteq K$. Then $\{K : F\} = [K : F]$ if and only if $\{K : E\} = [K : E]$ and $\{E : F\} = [E : F]$.*

Proof. Note that

$$\{K : F\} = \{K : E\}\{E : F\} \quad \text{and} \quad [K : F] = [K : E][E : F].$$

Therefore, the two quantites on the left hand side are equal if and only if the ones on the right hand side are equal to each other. □

This gives us a different way to characterize *finite* separable extensions.

Theorem 13.5. *Let E/F be a finite extension. Then $\{E : F\} = [E : F]$ if and only if E/F is separable.*

Proof. One direction is clear. To prove the other, let $\alpha \in E$, and consider $F \subseteq F(\alpha) \subseteq E$. Then $\{E : F\} = [E : F]$ gives $\{F(\alpha) : F\} = [F(\alpha) : F]$. Therefore, all roots of the minimal polynomial of α are distinct, and so E/F is separable. □

Definition 13.3. A field F is *perfect* if every finite extension of F is separable.

This is quite a strong condition to check, so we first need a lemma before we can give any example of perfect fields.

Lemma 13.6. *Let $f \in \overline{F}[X]$ be a monic polynomial and $f^n \in F[X]$ for some $n \geq 1$. Suppose that the characteristic of F does not divide n. Then $f \in F[X]$ instead.*

Proof. Write $f = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$ where $a_n = 1$, and suppose that $a_n, a_{n-1}, \ldots, a_{n-i-1}$ all belong to F for some $i \geq 1$. Consider the coefficient of X^{mn-i} in f^m; this is equal to

$$\sum_{k_1+k_2+\cdots+k_m=mn-i} a_{k_1} a_{k_2} \ldots a_{k_m}.$$

where $0 \leq k_i \leq n$. In particular, if $k_j = n - i$, then $k_{j'} = n$ for all $j' \neq j$. Therefore, this sum can be rewritten as

$$m a_{n-i} + \sum_{\substack{k_1+k_2+\cdots+k_m=mn-i \\ n-i<k_j\leq n}} a_{k_1} a_{k_2} \cdots a_{k_m}.$$

By the induction hypothesis, the sum on the right belongs to F, so $ma_{n-i} \in F$. Since $\operatorname{char} F$ does not divide m, m must be invertible, so it follows that $a_{n-i} \in F$. Therefore, we are done by induction. □

By using this lemma, we can now show that all the usual fields like $\mathbb{Q}$ and $\mathbb{R}$ are perfect.

Theorem 13.7. *Any field F of characteristic 0 is perfect.*

Proof. Suppose that $f \in F[X]$ is irreducible. Let α be a root of f in $\overline{F}$ with multiplicity k. Then

$$f = \prod_{i=1}^{n} (X - a_i)^k = \left(\prod_{i=1}^{n} (X - a_i) \right)^k = g^k.$$

However, by the above lemma $g \in F[X]$, so f is irreducible means that $k = 1$. In other words, f is separable. □

§ Lecture 14

It turns out that there is a general method to determine whether any polynomial is separable. The following section is taken from Aluffi's *Algebra: Chapter 0*.

Theorem 14.1. *Let $f \in F[X]$, and let f' be its formal derivative. Then f is separable if and only if* $\gcd(f, f') = 1$.

Proof. Suppose that a is a root of f in its splitting field E over F with multiplicity $k > 1$. Then there exists a polynomial $g \in E[X]$ such that

$$f = (X - a)^k g.$$

Then differentiation gives

$$f' = k(X - a)^{k-1} g + (X - a)^k g'.$$

Therefore, a is a root of f' as well. Consequently, the minimal polynomial of a over F divides both f and f', so it follows that $\gcd(f, f') \neq 1$.

Now suppose that $\gcd(f, f') = d$ where d is not a constant polynomial. Define E as before, and let a be a root of $d \in E$. Then

$$f = (X - a)g \implies f' = g + (X - a)g'.$$

Since $0 = f'(a) = g(a)$, it follows that g is also divisible by $X - a$. Therefore, a is a double root of f. □

In particular, this gives another method to show that all fields of characteristic 0 are perfect.

Another proof of theorem 13.7. Let F be a field with characteristic 0. Like above, it suffices to show that all irreducible polynomials in $F[X]$ are separable. Let f be such a polynomial. Then f' is non-zero since $\operatorname{char} F = 0$ and has degree less than f. Since f is irreducible, this means that $\gcd(f, f') = 1$, so f is separable. Therefore, any finite extension of F is separable, and hence F is perfect. □

How about fields of characteristic p? It turns out that we can completely characterize them!

Theorem 14.2. *A field of characteristic p is perfect if and only if the Frobenius endomorphism $\phi : a \to a^p$ is surjective.*

Proof. Let F be a field of characteristic p, and suppose that ϕ is not surjective. Then there exists $u \in F$ which is not in $\phi(F)$. Then $X^p - u$ has no roots in F. Let s be one of its roots in $\overline{F}$. Then

$$(X - s)^p = X^p - s^p = X^p - u,$$

so s is the only root of $X^p - u$. In particular, the minimal polynomial of s over F is not separable, so $F(s)$ is a finite but inseparable extension of F.

Now suppose that ϕ is surjective. Let $f \in F[X]$ be irreducible and inseparable polynomial. Then $\gcd(f, f') \neq 1$, so $f' = 0$. Since $F[X]$ has characteristic p, this means that $f = g(X^p)$ for some polynomial g. Then,

$$f = a_n(X^p)^n + \cdots + a_0 = (b_n X^n)^p + \cdots + b_0^p = (b_n X^n + \cdots + b_0)^p,$$

where $b_i^p = a_i$ for each i. This is impossible since f is irreducible. Therefore, every irreducible polynomial in $F[X]$ is separable, and hence any algebraic extension of F is separable. In other words, F is perfect. □

In particular, Theorem 14.2 directly gives us the following corollary.

Corollary 14.2.1. *Every finite field is perfect.*

Proof. The Frobenius homomorphism is a field homomorphism so it is injective. By finiteness, it is therefore surjective. □

§ Lecture 15

Today we will explore the main topic of this course: Galois correspondence. In the notes below, a *finite normal* extension is the one usually referred to as a *Galois* extension by other literature.

Definition 15.1. Let K be a finite extension of F. We say K is a finite normal extension if K is separable and a splitting field over F.

Note that this implies $[K : F] = \{K : F\}$ and every $\phi : \overline{F} \to \overline{F}$ fixing F also preserves K.

Theorem 15.1. *Let K/F be a finite normal extension. Let E be an intermediate field. Then K/E is also finite normal.*

Proof. K/E is separable since K/F is separable. Moreover, if K is a splitting field of a set $\mathcal{P}$ of polynomials over F, then it is also a splitting field of the same set of polynomials over E. □

Here is a very useful theorem regarding finite normal extenions (which makes them very nice.)

Theorem 15.2. *Given a finite normal field extension K/F, and an intermediate field E,*

$$\{\phi : E \to K \text{ fixing } F\} \Leftrightarrow \{\text{left cosets of } G(K/E) \text{ in } G(K/F)\}.$$

Proof. Just mindless checking. □

We will see that if E/F is normal (which does not always happen!) then $G(K/F)$ is a normal subgroup of $G(K/F)$, and this becomes an isomorphism of groups.

§ Lecture 16

Finally, we can now state the main theorem of this course.

Theorem 16.1 (Fundamental Theorem of Galois Theory)**.** *Let K/F be a finite normal extension. Then the map λ mapping*

$$\{F \leq E \leq K\} \longrightarrow \{H \subseteq G(K/F)\}.$$

which sends E to the subgroup $G(K/E)$ is an order reversing bijection. To be more specific, λ satisfies the following:

1. *E is the fixed field of $\lambda(E) = G(K/E)$.*
2. *For any subgroup $H \subseteq G(K/F)$, if E is the fixed field of H, then $\lambda(E) = H$.*
3. *$[K : E]$ is equal to $|G(K/E)|$, and $[E : F]$ is equal to $[G(K/F) : G(K/E)]$.*
4. *E/F is a finite normal extension if and only if $\lambda(E)$ is normal in $G(K/F)$.*

Proof. This looks quite intimidating but it is just definition chasing.

1. Let $K_{\lambda(E)}$ be the subfield of K fixed by the elements of $\lambda(E)$. By definition, E is a subset of $K_{\lambda(E)}$. Now let α be an element of K which is not contained in E. Since K is a finite normal extension of E, it contains all conjugates of α, and there are at least 2 including α since α is separable and has degree at least 2. Let β be a different conjugate. We can construct an isomorphism $\phi : E(\alpha) \to E(\beta)$ which fixes E and extend it to an isomorphism of $\phi' : K \to K$. Then $\phi' \in G(K/E)$, but ϕ' does not fix α. Therefore, $\alpha \notin K_{\lambda(E)}$.

2. Again, by definition, $H \subset \lambda(E) = \lambda(K^H)$. Consider K/E. This is a finite separable extension, so it has a primitive element, say α, such that $K = E(\alpha)$. Let n be the degree of α over K^H. In fact, K/E is a finite normal extension, so $|\lambda(E)| = |G(K/E)| = [K : E] = n$. Therefore, it suffices to show that H also has size n. Now consider

$$f(x) = \prod_{g \in H} (x - g(\alpha)) \in K[x].$$

   If $h \in H$ is any automorphism in H, then

$$h(f(x)) = \prod_{g \in H} (x - h(g(\alpha)) = \prod_{g' \in H} (x - g'(\alpha)) = f(x).$$

   Hence in fact, $f \in E[x]$. Therefore, f is divisible by the irreducible polynomial of α, so f has degree at least n, and hence $|H| \geq n$. Combined with the fact that $H \subset \lambda(E)$ shows that $H = \lambda(E)$ as desired.

3. This follows by Theorem 15.2.

4. E/F is a finite normal extension if it is separable and a splitting field. However, separability is given since it is a subextension of a separable extension. Therefore, it suffices to show that E is a splitting field over F iff $\lambda(E)$ is a normal subgroup. Let $f(x) \in F[X]$ be an irreducible polynomial, and suppose that it has a root α in E. Suppose that $\lambda(E)$ is normal. We do know that the other roots of f lie in K. Let β be one such root. Then there exists an automorphism $g \in G(K/F)$ such that $g(\alpha) = \beta$. Therefore, our goal now is to show that $g(\alpha) \in E$ for all α in E and for any $g \in G(K/E)$.

By 2, it suffices to show that $g(\alpha)$ is fixed by all the elements of $\lambda(E)$. Let h be an element of $\lambda(E)$. Then $g^{-1}hg(\alpha) = \alpha$ by normality of $\lambda(E)$, so $h(g(\alpha)) = g(\alpha)$. Similarly, if $\lambda(E)$ is not normal, we can find an element $h' \in \lambda(E)$, $g' \in G(K/F)$ and $\alpha \in E$ such that $g(\alpha) \notin E$. In other words, E is not a splitting field, so E is not normal. This shows that the normality of the field extension and the normality of the subgroup are equivalent as required.

Now let's prove part ii. Let E/F be an intermediate extension which is also normal. Then any element of $G(K/F)$ preserves E, hence the restriction map defines an element of $G(E/F)$. This map is surjective since for any automorphism $\tau \in G(E/F)$ we can create an automorphism τ' of K/F which restricts to τ using the primitive element theorem and isomorphism extension theorems. The kernel of this homomorphism is exactly the group $G(K/E)$, so

$$G(E/F) \cong \frac{G(K/F)}{G(K/E)}.$$ □

§ Lecture 17

Example 17.0.1. Let's compute the Galois group of the splitting field of $x^4 - 2 \in \mathbb{Q}[x]$. Let K denote the splitting field. This polynomial is irreducible in $\mathbb{Q}[x]$ due to Eisenstein's criterion. The roots of are $\alpha \coloneqq \sqrt[4]{2}$, $-\alpha$, $i\alpha$ and $-i\alpha$. Moreover, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ and $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$ (it cannot be 1 since $i \notin \mathbb{Q}(\alpha)$.). Therefore, $[K : \mathbb{Q}] = 8$.

Now, any element $g \in G(K/\mathbb{Q})$ is determined by its actions on α and i, and it must send them to their respective conjugates. There are in total 8 possible options for g, so it follows that every one of these options can actually be realized. It is then easy to see that $G(K/\mathbb{Q})$ is D_4.

Example 17.0.2. Now let's compute the Galois group of $x^5 - 2 \in \mathbb{Q}[x]$. The splitting field of this polynomial is $K \coloneqq \mathbb{Q}(\sqrt[5]{2}, \omega)$, where $\alpha = \sqrt[5]{2}$ and ω is a primitive fifth root of unity. Now $\deg(\alpha) = 5$ and $\deg(\omega) = 4$, so $[K : \mathbb{Q}] \geq 20$. This shows that $[K : \mathbb{Q}] = 20$. Again, using the same argument as above shows that $G(K/\mathbb{Q})$ consists of all 20 possible automorphisms.

Let $\tau : K \to K$ such that $\tau(\alpha) = \zeta\alpha$ and $\tau(\omega) = \omega$, and let σ be such that $\sigma(\alpha) = \alpha$ and $\tau(\omega) = \omega^2$. Then we can check that τ and σ generate $G(K/\mathbb{Q})$ and that $\tau\sigma = \sigma^2\tau$. To be more specific,

$$G(K/\mathbb{Q}) = \{\sigma^k\tau^\ell \mid 0 \leq k \leq 4, 0 \leq \ell \leq 3, \sigma^5 = \tau^4 = e, \tau\sigma = \sigma^2\tau.\}$$

Then the multiplication rule is given by

$$\sigma^a\tau^b \cdot \sigma^c\tau^d = \sigma^{a+2^b c}\tau^{b+d}.$$

Example 17.0.3. Let's find the Galois group of $x^6 - 2$! Again, $G(K/\mathbb{Q})$ has degree 12 over $\mathbb{Q}$, and it is generated by $\alpha = \sqrt[6]{2}$ and $\zeta = e^{\frac{2\pi i}{6}}$. It is easy to check that $G(K/\mathbb{Q}) = D_6$ in this case.

§ Lecture 18

Let F be a field, and let $F[y_1, \ldots, y_n]$ be the ring of polynomials in n variables. Let $F(y_1, \ldots, y_n)$ be its field of fractions. The group S_n acts on $F[y_1, \ldots, y_n]$ by permuting the n indeterminates.

Definition 18.1. $f \in F[y_1, \ldots, y_n]$ is symmetric if it is fixed by all the elements of S_n.

Note that these polynomials, namely the set $F[y_1, \ldots, y_n]^S$, forms a ring. Of course, this is a vector space over F, but the basis is quite complicated and it does not reveal anything about the structure of the ring. Instead, it is more instructive to find its generators as a K-algebra.

Let $S = F(y_1, \ldots, y_n)^{S_n}$. Let $f(x) = \prod_{i=1}^{n}(x - y_i)$. If we expand this product,

$$f(x) = \sum_{i=0}^{n}(-1)^{n-1}e_{n-i}x^i,$$

where e_{n-i} is the elementary symmetric polynomial of degree $n - i$.

Consider the field extension $F(y_1, \ldots, y_n)/S$. From the above, we have that $f \in s[x]$. In fact, it is easy to see that $F(y_1, \ldots, y_n)$ is the splitting field of f over S. Therefore, this is a finite normal extension, and so the Galois group of this extension is S_n. Since any subgroup H of S_n can be realized as a Galois group of an intermediate field extension and any finite group can be embedded in S_n, it follows that we can always construct a finite normal extension with any finite group as its Galois group.

§ Lecture 19

Moreover, we also have the following theorem, often called the fundamental theorem of symmetric polynomials.

Theorem 19.1. *With notation as above, $S = F(e_1, \ldots, e_n)$.*

Proof. Let $E = F(e_1, \ldots, e_n)$. Obviously, $E \subseteq S$. Since each permutation of the interdeterminates form an automorphism of $F(y_1, \ldots, y_n)$ over S, it follows that $[F(y_1, \ldots, y_n) : S] \geq |G(F(y_1, \ldots, y_n)/S)| \geq n!$. (In general, $|G(E/F)| = [E : E^G]$, so it divides $[E : F]$.) On the other hand, $F(y_1, \ldots, y_n)$ is the splitting field of the polynomial

$$f(x) = \prod_{i=1}^{n}(x - y_i) \in E[x],$$

so the degree $[F(y_1, \ldots, y_n) : E] \leq n!$. Therefore, this gives us

$$n! \leq [F(y_1, \ldots, y_n) : S] \leq [F(y_1, \ldots, y_n) : E] \leq n!,$$

and thus, $E = S$ as desired. □

In particular, this shows that any symmetric expression of the roots of a polynomial can be expressed as a polynomial of the coefficients.

Definition 19.1. Let $f(x) \in F[x]$, with roots $\alpha_1, \ldots, \alpha_n$. The *discriminant* of f is defined to be Δ^2, where

$$\Delta = \prod_{i<j}(\alpha_i - \alpha_j).$$

Note that the discriminant is also equal to

$$\Delta^2 = \prod_{i \neq j}(\alpha_i - \alpha_j).$$

Lemma 19.2. *The discriminant is an element of F.*

Proof. Note that Δ^2 is a symmetric expression of $\alpha_1, \ldots, \alpha_n$. Therefore, it can be written as a polynomial of the coefficients, which are all in F. Therefore, the discriminant is also in F. □

Theorem 19.3. *Let $f \in F[x]$ be a polynomial. If $\Delta \in F$ (i.e., the discriminant is a square), then the galois group of f is a subgroup of A_n.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f, and suppose that $\sigma \in S_n$ acts by $\sigma(\alpha_i) = \alpha_{\sigma(i)}$. Then in general,

$$\sigma(\Delta) = \operatorname{sgn}(\sigma) \cdot \Delta.$$

Therefore, $\Delta \in F$ iff Δ is fixed by the elements of $G(K/F)$ iff $\operatorname{sgn}(\Delta) = 1$ for each $\sigma \in G(K/F)$. This occurs if and only if $G(K/F) \subset A_n$. □

Now let's explore cyclotomic polynomials and cyclotomic extensions!

Definition 19.2. Let F be a field. The nth cyclotomic extension of F is the splitting field of $x^n - 1$ over F.

In the following, we will assume that F is infinite and that $\operatorname{char}(F)$ does not divide n.

Lemma 19.4. *With the assumptions above, $x^n - 1$ is separable over F.*

Proof. Let α be the root of $x^n - 1$. Then

$$\frac{x^n - 1}{x - \alpha} = x^{n-1} + x^{n-2}\alpha + \cdots + \alpha^{n-1}.$$

Evaluating this polynomial at α gives $n\alpha^{n-1} \neq 0$, so α is not a double root of this polynomial. Therefore, $x^n - 1$ is separable. (We can also show this by noting that $\gcd(x^n - 1, nx^{n-1}) = 1$ as long as $\operatorname{char}(F)$ does not divide n.) □

A corollary of this is that the nth cyclotomic extension is finite normal. We will now restrict our attention to the cyclotomic extensions of $\mathbb{Q}$, and in particular, the case when n is prime.

Theorem 19.5. *Let p be a prime. Then $\frac{x^p-1}{x-1}$ is irreducible in $\mathbb{Q}[x]$.*

Proof. Let g denote the given polynomial. Then

$$g(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{i=0}^{p-1} \binom{p}{i} x^{p-i-1}.$$

Since $\binom{p}{i}$ is divisible by p except when $i = p$, by Eisenstein's Criterion it follows that $g(x+1)$ is irreducible. Consequently, g is also irreducible. □

Therefore, the pth cyclotomic extension over $\mathbb{Q}$ has degree $p - 1$. Let

$$\Phi_p(x) \coloneqq x^{p-1} + x^{p-2} + \cdots + 1.$$

This is called the cyclotomic polynomial of order p. (Later, we will see how to define this for all positive integers n.)

Let's compute the Galois group of the pth cyclotomic extension, say K. Let $\zeta = e^{\frac{2\pi i}{p}}$ be a root of Φ_p. Then the automorphisms of K over $\mathbb{Q}$ are precisely the ones mapping ζ to ζ^k where $1 \leq k \leq p - 1$. Moreover, composition is the same as multiplying the powers and taking the remainder mod p. Therefore, the Galois group $G(K/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/(p-1)\mathbb{Z}$.

Now we tackle the case when n is not prime.

Definition 19.3. The nth cyclotomic polynomial is defined to be the polynomial

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} (x - \zeta_k),$$

where $\zeta_k = e^{\frac{2\pi i k}{n}}$.

Note that ζ_k have multiplicative order n precisely when $\gcd(k, n) = 1$. These are called the *primitive* roots of unity. Therefore, in other words, the cyclotomic polynomial Φ_n is the polynomial having each primitive root of unity as its root exactly once and nothing else.

We first show that the nth cyclotomic polynomial indeed belongs to $\mathbb{Q}[x]$. In fact, a stronger statement is true.

Theorem 19.6. *$\Phi_n(x)$ is an irreducible monic polynomial in $\mathbb{Z}[x]$.*

Proof. Let K be the nth cyclotomic extension. Then any automorphism $\sigma \in G(K/\mathbb{Q})$ take the primitive nth roots of unity to primitive nth roots of unity. Therefore, It permutes the roots of $\Phi_n(x)$, and hence $\Phi_n(x) \in \mathbb{Q}[x]$.

To see that it is in fact inside $\mathbb{Z}[x]$, note that it divides $x^n - 1$, and any rational polynomial dividing a monic polynomial with integer coefficients must itself have integer coefficients as well.

The irreducibility is much harder to prove. One proof can be found in *Algebra: Chapter 0*. □

This gives us an easy way to characterize the Galois group of the nth cyclotomic extension for any positive integer n.

Theorem 19.7. *Let K be the nth cyclotomic extension. Then $K \cong \mathbb{Q}[x]/\Phi_n(x)$, and $G(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof. Let $\zeta = e^{\frac{2\pi i}{n}}$. Then any element of $G(K/\mathbb{Q})$ must send ζ to ζ^k where $\gcd(k, n) = 1$, and these are the only elements of $G(K/\mathbb{Q})$. Therefore, $G(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. □

§ Lecture 20

It is now time for the finale of the course. In the remainder, we are going to prove the Abel-Ruffini theorem, more commonly known as the unsolvability of the quintic by radicals.

Theorem 20.1. *A polynomial f is solvable by radicals if and only if the Galois group of f is a* solvable *group.*

We will first define what a solvable group is.

Definition 20.1. Let G be a finite group. The subnormal series of G is a sequence of subgroups

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_n = G,$$

of subgroups, such that G_i is normal in G_{i+1}.

Definition 20.2. The *factor groups* of a subnormal series are $H_{i+1} = G_{i+1}/G_i$.

Example 20.2.1. Let $G = D_n$, the dihedral group of order $2n$. Then let G_1 be the subgroup generated by rotations; it is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Then we have the subnormal series $\{e\} \subset G_1 \subset D_n$. The factor groups are $H_1 = G_1$ and $H_2 = \mathbb{Z}/2\mathbb{Z}$.

Definition 20.3. Let G be a finite group. A composition series is a subnormal series

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_n = G,$$

where G_{i+1}/G_i is simple, i.e., its only normal subgroups are the trivial subgroup and the whole group itself.

Example 20.3.1. The composition series of $G = S_3$ would be $\{e\} \subset \mathbb{Z}/3\mathbb{Z} \subset S_3$, since the factor groups are $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$ which are both simple.

In general, there can be many composition series for a finite group G. However, the following theorem says that they are essentially *equivalent*.

Theorem 20.2 (Jordan-Holder). *For a finite group G, any two composition series give the same list of factor groups up to reordering.*

Finally, here is a definition of a solvable group.

Definition 20.4. A *solvable* group is a group with a composition series with abelian factors.

Note that solvability of a group is well-defined by the Jordan-Holder theorem. Moreover, in order to show that a group is not solvable, we just need to find a composition series one of whose factors is not abelian.

Question. Show that S_5 has composition series $\{e\} \subset A_5 \subset S_5$.

Definition 20.5. $f(x) \in F[x]$ is solvable by radicals if it splits in an extension E/F, where $E = F(\alpha_1, \ldots, \alpha_k)$, and $\alpha_i^{p_i} \in F(\alpha_{i-1})$ for all $1 \leq i \leq n$.

It is easy to see that this coincides with the usual notion of solvability. We will now prove Theorem 20.1 in multiple steps.

Lemma 20.3. *Let E/F be the splitting field of $f(x) = x^n - a$ where $a \in F$, and F is a perfect field. Then $G(E/F)$ is solvable.*

Proof. We will first consider the case when F contains all nth roots of unity. Let α be a root of f, and let ζ be a primitive nth root of unity. Then $\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha$ are roots of $x^n - a$. Therefore, $E = F(\alpha)$. Given g in the galois group, $g(\alpha) \in \{\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha\}$, and g is fully determined by its value on α. Therefore, it follows that $G(E/F)$ is a subgroup of $\mathbb{Z}/n\mathbb{Z}$. In particular, it is abelian, so solvable.

Now consider the case when F does not contain all roots of unity. Again, let ζ be a primitive root of unity, and consider $F \subset F(\zeta) \subset E$. Then $G(F(\zeta)/F)$ is abelian, and by case 1, $G(E/F(\zeta))$ is also abelian. Note that $F(\zeta)/F$ is finite normal since it is the splitting field of $x^n - 1$. Therefore, it follows that $G(E/F(\zeta))$ is normal in $G(E/F)$. Now we can construct a subnormal series as follows:

$$\{e\} \subset G(E/F(\zeta)) \subset G(E/F).$$

Then both factor groups are abelian, so it follows that $G(E/F)$ is solvable. □

Now we are ready to prove Theorem 20.1.

Proof. First, consider $E_1 = F(\alpha_1)/F$. Let L_1/F be teh splittting field of $x^{p_1} - \alpha_1^{p_2}$. Then $F \subset E_1 \subset L_1$ and by the previous theorem, $G(L_1/F)$ is solvable.

Now let

$$f(x) = \prod_{\sigma \in G(E/F)} (x^{p_2} - \sigma(\alpha_2)^{p_2}) \in F[x].$$

Let L_2 be the splitting field of f over L_1. Then L_2/F is a normal extension, so $G(E/L_2) \subset G(E/F)$ is a normal subgroup...

□

This shows that solvable polynomials have solvable Galois groups. It's also true that if a polynomial has a solvable Galois group, then it is solvable by radicals.

Therefore, our final goal is to find a polynomial with a non-solvable Galois group. We know that S_5 is not solvable, so let's try to find a polynomial with Galois group S_5. Let $f(x)$ be a degree 5 irreducible polynomial in $\mathbb{Q}[x]$, and let K be its splitting field over $\mathbb{Q}$. Then $5 \mid \deg K = |G(K/\mathbb{Q})| \mid 5!$. Therefore, by Cauchy's theorem, $G(K/\mathbb{Q})$ contains an element of order 5, i.e, a 5-cycle. Therefore, it suffices to find f such that $G(K/\mathbb{Q})$ also contains a 2-cycle, since a 5-cycle and a 2-cycle together generates S_5. Note that this can be done by finding f such that f has 3 real roots and 2 complex roots, since complex conjugation would give the 2-cycle that we need.

Now convince yourself by Desmos that $f(x) = 2x^5 - 5x^4 + 5$ has exactly 3 real roots. Therefore, this polynomial is not solvable by radicals!