MA 5C LECTURE NOTES

ZAVOSH AMIR-KHOSRAVI

Abstract. These are lecture notes for Ma 5c taught at Caltech during the Spring quarter of 2018. The content and order of the material largely follows Dummit and Foote, though they do occasionally diverge.

1. Lecture 1

We recalled fields and the basics of field extensions, corresponding roughly to 13.1 from Dummit and Foote.

2. Lecture 2

Theorem 2.1. *Let K/F be a field extension, $p(X) \in F[X]$ an irreducible polynomial, $\alpha \in K$ a root of $p(X)$, and $F(\alpha)$ the subfield of K generated by α over F. The map*

$$e_\alpha : F[X]/(p(X)) \to F(\alpha), \quad e_\alpha(q(X)) = q(\alpha)$$

is an isomorphism.

Proof. The left-hand side is a field since $p(X)$ is irreducible. e_α is non-zero, therefore it's injective. Then the image of e_α is a subfield of K, contained in $F(\alpha)$, that contains $e_\alpha(X) = \alpha$. Since $F(\alpha)$ is the minimal such field, e_α must be surjective. □

Example 1

Consider the polynomial $p(x) = x^4 + x^3 + x^2 + x + 1$. It is irreducible over $\mathbb{Q}$. To see this, note $p(x) = (x^5 - 1)/(x - 1)$, and apply Eisenstein's criterion to $p(x + 1)$.

Last time we constructed a field $F = \mathbb{Q}[x]/(p(x))$ which $p(x)$ has a root. On the other hand, $\zeta_5 = e^{2\pi i/5} \in \mathbb{C}$ is a root of $p(x)$, so the subfield $\mathbb{Q}(\zeta_5) \subset \mathbb{C}$ generated by ζ_5 over $\mathbb{Q}$, is also an extension of $\mathbb{Q}$ containing a root of $p(x)$. The theorem shows that F and $\mathbb{Q}(\zeta_5)$ are isomorphic.

Example 2

Let $F_1 = \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, $F_2 = \mathbb{Q}(\zeta_3\sqrt[3]{2}) \subset \mathbb{C}$. Both $\sqrt[3]{2}$ and $\zeta_3\sqrt[3]{2}$ are roots of $x^3 - 2$, which is irreducible over $\mathbb{Q}$. By the theorem, F_1 and F_2 are both isomorphic to $F[X]/(x^3 - 2)$. In particular, they are isomorphic to each other!

A slightly more general form of this theorem will come in handy later.

Theorem 2.2. *Let K/F, K'/F' be field extensions, and $\phi : F \to F'$ an isomorphism. Suppose $\alpha \in K$ is a root of an irreducible $p(X) \in F[X]$, and $\beta \in K'$ is a root of $q(X) = \phi(p(X)) \in F'[X]$. The ϕ extends to an isomorphism $\widetilde{\phi} : F(\alpha) \to F'(\beta)$ such that $\widetilde{\phi}(\alpha) = \beta$ and $\widetilde{\phi}|_F = \phi$.*

Proof. The map $\phi : F \to F'$ which extends to $\Phi : F[X] \to F'[X]$ induces an isomorphism

$$\psi : F[X]/(p(X)) \to F'[X]/(q(X))$$

By Theorem 2.1, the map $\phi_1 : F[X]/(p(X)) \to F(\alpha)$ sending X to α is an isomorphism, as is the map $\phi_2 : F'[X]/(q(X)) \to F'(\beta)$ sending X to β. Then

$$\widetilde{\phi} : \phi_2 \circ \psi \circ \phi_1^{-1} : F(\alpha) \to F'(\beta)$$

is an isomorphism that sends α to β, and restricts to ϕ on F. □

Algebraic Extensions

Let K/F be a field extension. An element $\alpha \in K$ is said to be *algebraic over* F, if $p(\alpha) = 0$ for some non-zero $p(X) \in F[X]$. If every element of K is algebraic over F, K itself is an *algebraic extension* of F. An element $\alpha \in K$ is called *transcendental* over F, if it's not algebraic. If K/F contains any trancendental element over F, it's called a transcendental extension of F.

Examples

- Let k be a field. The field of rational functions $k(X)$ in variable X is a transcendental extension of k.
- The field $\mathbb{Q}(\pi)$ generated by $\pi \in \mathbb{R}$ over $\mathbb{Q}$ is transcendental, because π is not the root of any polynomial. Therefore $\mathbb{Q}(\pi)/\mathbb{Q}$ is transcendental.
- $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$ is algebraic over $\mathbb{Q}$, since it's a root of $X^3 - 2$. But is the entire extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ algebraic? We have to understand algebraicity better to answer this.

Proposition 2.3. *Let K/F be an extension, $\alpha \in K$ algebraic over F. Then there is a unique monic irreducible polynomial $m_\alpha(X) \in F[X]$ having α as root.*

Proof. Consider the map

$$F[X] \to F(\alpha), \quad f(X) \mapsto f(\alpha).$$

Its kernel is a maximal ideal $\mathfrak{m} \subset F[X]$. Since $F[X]$ is a PID, $\mathfrak{m} = (p(X))$ for some polynomial $p(X)$. Since $F[X]^\times = F$, all the possible generators of $\mathfrak{m}$ are of the form $cp(X)$ for $c \in F^\times$. There is therefore a unique *monic* generator $m(X)$ of $\mathfrak{m}$. It's irreducible since $\mathfrak{m}$ is maximal.

Let $p(X) \in F[X]$ be any polynomial such that $p(\alpha) = 0$. Then $p(X) \in \mathfrak{m}$, so $p(X) = m(X)q(X)$ for some $q(X)$. If $p(X)$ is irreducible, $q(X)$ must be a unit q. If $p(X)$ is further monic, $q = 1$, therefore $p(X) = m(X)$. □

Corollary 2.4. *Let K/F be an extension, $\alpha \in K$ algebraic. Then $[F(\alpha) : F] = \deg m_\alpha(X)$.*

Proof. By Theorem 2.1, $F(\alpha) \cong F[X]/(m_\alpha(X))$.

Then as we saw before $F(\alpha)$ has F-basis $\{1, \alpha, \alpha^2, \cdots, \alpha^{d-1}\}$, where $d = \deg m_\alpha(X)$. □

Definition 2.5. If $\alpha \in K$ is algebraic over F, the unique monic irreducible polynomial $m_\alpha(X) \in F[X]$, which has α as a root is called the the *minimal polynomial* of α over F. The *degree* of α over F is the degree of its minimal polynomial.

For example, the number $i \in \mathbb{C}$ has degree 2 over $\mathbb{Q}$, since its minimal polynomial is $x^2 + 1$.

Proposition 2.6. *Let $\alpha \in K$, K a field over F. Then α is algebraic over F if and only if $F(\alpha)/F$ is a finite extension.*

Proof. If α is algebraic, then $F(\alpha) = F[X]/(m_\alpha(X))$, so $F(\alpha)/F$ is finite, having degree $m_\alpha(X)$.

Suppose $F(\alpha)/F$ is a finite extension. Then $T : F(\alpha) \to F(\alpha)$, $T(x) = \alpha x$ is a linear operator on a finite-dimensional F-vector space. Let $m(X)$ be the minimal polynomial of T. On the one hand $m(T) = 0$, on the other hand $m(T)$ is the operator $x \mapsto m(\alpha)x$, so $m(\alpha) = 0$, and α is algebraic over F. □

Corollary 2.7. *The simple extension $F(\alpha)/F$ is algebraic if and only if α is algebraic over F.*

Proof. If $F(\alpha)/F$ is an algebraic extension, then $\alpha \in F(\alpha)$ is certainly algebraic. Now suppose α is algebraic. By the proposition $F(\alpha)/F$ is finite. Let $\beta \in F(\alpha)$ be arbitrary. The field $F(\beta)$ is an F-subspace of $F(\alpha)$ so $[F(\beta) : F] \leq [F(\alpha) : F] < \infty$. Then β is algebraic by the proposition, so the entire extension $F(\alpha)/F$ is algebraic. □

Corollary 2.8. *A finite extension K/F is algebraic.*

Proof. Suppose $\alpha \in K$, K/F finite. Since $F(\alpha) \subseteq K$, $\dim_F F(\alpha) \leq \dim_F K < \infty$, so $F(\alpha)/F$ is finite. By the proposition, α is algebraic. Since this is true for all $\alpha \in K$, K/F itself is an algebraic extension. □

Now we know that $\mathbb{Q}(\sqrt[3]{2})$ is an algebraic extension of $\mathbb{Q}$, so any element of it is algebraic, say $\alpha = (\sqrt[3]{2} + \sqrt[3]{4})^{-1}$. We also know that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Now $[\mathbb{Q}(\alpha) : \mathbb{Q}] \neq 1$, since that would imply $\mathbb{Q}(\alpha) = \mathbb{Q}$ and $\alpha \notin \mathbb{Q}$. Is it possible that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$?

3. Lecture 3

Theorem 3.1. *Let $F \subseteq K \subseteq L$ be fields. Then*

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

Proof. Let $S = \{\alpha_i\}_{i \in I}$ be an F-basis for K, and $T = \{\alpha_j\}_{j \in J}$ be a K-basis for L. We claim $\{\alpha_i \beta_j\}_{(i,j) \in I \times J}$ is an F-basis for L. First we show it's linearly independent.

Suppose $\sum_{i,j} c_{i,j} \alpha_i \beta_j = 0$, for some $c_{i,j} \in F$ (almost all zero). Then we can write

$$\sum_{i,j} c_{i,j} \alpha_i \beta_j = \sum_{i \in I} \left(\sum_{j \in J} c_{i,j} \beta_j \right) \alpha_i = 0.$$

Then for each i, $\sum_{j \in J} c_{i,j} \beta_j \in K$. Since $\{\alpha_i\}_{i \in I}$ is an F-basis for K, for each i

$$\sum_{j \in J} c_{i,j} \beta_j = 0.$$

Now since $\{\beta_j\}_{j \in J}$ is linearly independent, the above shows $c_{i,j} = 0$ for all j, and all i.

A similar argument shows $\{c_{i,j}\}_{(i,j) \in I \times J}$ spans L over F, hence it's a basis. Then

$$[L : F] = |I \times J| = |I| \cdot |J| = [K : F][L : K].$$

□

Let's apply this theorem to $L = \mathbb{Q}(\sqrt[3]{2})$, $F = \mathbb{Q}$. Suppose K is *any* subextension of L over $\mathbb{Q}$. The theorem shows $[K : \mathbb{Q}]$ divides $[L : \mathbb{Q}] = 3$. Then either $[K : \mathbb{Q}] = 3$ or $[K : \mathbb{Q}] = 1$. Therefore if $K \neq \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$. In other words, there are no fields lying strictly between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt[3]{2})$. For example, $\mathbb{Q}((\sqrt[3]{2} + \sqrt[3]{4})^{-1}) = \mathbb{Q}(\sqrt[3]{2})$ necessarily.

Definition 3.2. A field extension K/F is *finitely generated* if $F = (\alpha_1, \cdots, \alpha_r)$ for finitely many $\alpha_i \in K$.

Lemma 3.3. *Let K/F be an extension, $\alpha_1, \cdots, \alpha_r \in K$. Define extensions*

$$F = F_0 \subseteq F_1 \subseteq F_1 \subseteq \cdots F_r$$

by $F_{i+1} = F_i(\alpha_i)$. Then $F_r = F(\alpha_1, \cdots, \alpha_r)$.

Proof. We proceed by induction. The base case $r = 1$ is trivial.

Suppose $F_i = F(\alpha_1, \cdots, \alpha_i)$ for all $1 \leq i < k$. We show it holds for $i = k$.

We have

$$\left.\begin{array}{r} \alpha_1, \cdots, \alpha_{k-1} \in F_{k-1} \subseteq F_k \\ \alpha_k \in F_k \end{array}\right\} \Longrightarrow \alpha_1, \cdots, \alpha_k \in F_k \Longrightarrow F(\alpha_1, \cdots, \alpha_k) \subseteq F_k.$$

By assumption $F_{k-1} = F(\alpha_1, \cdots, F_{\alpha_{k-1}})$, so conversely,

$$\left.\begin{array}{r} F_{k-1} = F(\alpha_1, \cdots, \alpha_{k-1}) \subseteq F(\alpha_1, \cdots, \alpha_k) \\ \alpha_k \in F(\alpha_1, \cdots, \alpha_k) \end{array}\right\} \Longrightarrow F_k = F_{k-1}(\alpha_k) \subseteq F(\alpha_1, \cdots, \alpha_k).$$

Since each is contained in the other, $F_k = F(\alpha_1, \cdots, \alpha_k)$. By induction, $F_r = F(\alpha_1, \cdots, \alpha_r)$. □

Theorem 3.4. *An extension K/F is finite $\iff$ $K = F(\alpha_1, \cdots, \alpha_r)$ for some $\alpha_i \in K$ that are algebraic over F.*

Proof. ($\Longrightarrow$:) If K/F is finite, then it is algebraic. If $\alpha_1, \cdots, \alpha_r$ are a basis, then $K = \mathrm{Span}_F\{\alpha_i\} \subseteq F(\alpha_1, \cdots, \alpha_r) \subseteq K$, so $K = F(\alpha_1, \cdots, \alpha_r)$ and K is generated by finitely many elements that are algebraic over F.

($\Longleftarrow$:) Let $F_0 = F$, $F_i = F_{i-1}(\alpha_i)$ for $i \geq 1$. Each α_i is algebraic over F, hence algebraic over F_{i-1}, hence $F_i = F_{i-1}(\alpha_i)$ is finite over F_{i-1}. Then

$$[K : F] = [F_r : F] = [F_r : F_{r-1}][F_{r-1} : F_{r-2}] \cdots [F_1 : F] \leq \infty.$$

□

Corollary 3.5. *Let K/F be a field extension. The elements $\alpha \in K$ that are algebraic over F form a subfield of K.*

Proof. Let L denote the set of $\alpha \in K$ that are algebraic over F. We have $F \subseteq L$, since each $a \in F$ is a root of $X - a \in F[X]$. In particular, $0, 1 \in L$. Then to show L is a subfield of K we only need to prove it is closed under addition, multiplication, and division (by non-zero elements). The rest of the field axioms are automatic, since they are the same as for K.

Let $\alpha, \beta \in K$ be algebraic over F. Then $F(\alpha, \beta)/F$ is an algebraic extension by the theorem, therefore $F(\alpha, \beta) \subseteq L$. In particular, $\alpha \pm \beta$, $\alpha \cdot \beta$, and α/β (when $\beta \neq 0$) are all in L. □

Example

Let $\overline{\mathbb{Q}} \subset \mathbb{C}$ be the subset of all numbers that are algebraic over $\mathbb{Q}$. By the corollary, this is a field. It's an algebraic extension of $\mathbb{Q}$ containing the roots of *all* irreducible polynomials over $\mathbb{Q}$. In particular, it contains all finite extensions of $\mathbb{Q}$ and is itself of infinite degree. Algebraic number theory is to a large extent the study of the extension $\overline{\mathbb{Q}}/\mathbb{Q}$.

We now have a basic understanding of algebraic extensions K/F. Next we want to investigate how different algebraic extensions interact. One possibility is an extension of an extension:

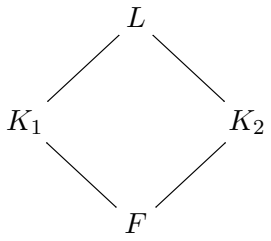
Lemma 3.6. *Suppose $F \subseteq K \subseteq L$ are fields, and K/F is algebraic. If $\alpha \in L$ is algebraic over K, it's also algebraic over F.*

Proof. Let $m_\alpha(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$ be the minimal polynomial of α over K. Since K/F is algebraic, c_i are algebraic over F, and so $F' = F(c_0, \cdots, c_{n-1})$ is a finite extension of F by Theorem 3.4. Since $m_\alpha(X)$ is irreducible over K, and $F' \subseteq K$, it's also irreducible over F'. Then $F'(\alpha) \simeq F'[X]/(m_\alpha(X))$ and $[F'(\alpha) : F'] = n$. We then have $[F'(\alpha) : F] = [F'(\alpha) : F'][F' : F] < \infty$, so $F'(\alpha)/F$ is finite, hence algebraic by Corollary 2.8. In particular, α is algebraic over F. □

Corollary 3.7. *Suppose $F \subseteq K \subseteq L$ are fields, and K/F, L/K are algebraic extensions. Then L/F is algebraic.*

Proof. L/K is algebraic, so any $\alpha \in L$ is algebraic over K. By the lemma it's algebraic over F. □

Another possible situation is an extension with two subextensions.



Here we may consider a third subextension of L/F generated by K_1 and K_2.

Definition 3.8. Let K_1/F and K_2/F be subextensions of some L/K. By K_1K_2 we denote the smallest subfield of L containing both K_1 and K_2. It is called the *amalgam* or *composite* of K_1 and K_2 in L.

For example if $K_1 = F(\alpha_1, \cdots, \alpha_r)$, $K_2 = F(\beta_1, \cdots, \beta_s)$, then $K_1K_2 = F(\alpha_1, \cdots, \alpha_r, \beta_1, \cdots, \beta_s)$.

More concretely, let $K_1 = \mathbb{Q}(\sqrt{a})$ and $K_2 = \mathbb{Q}(\sqrt{b})$, where $a, b \in \mathbb{Q}$. Considering K_1, K_2 as subfields of $\mathbb{C}$, we have $K_1K_2 = \mathbb{Q}(\sqrt{a}, \sqrt{b})$.

Proposition 3.9. *Let K_1/F and K_2/F be extensions, of possibly infinite degree, contained in a larger field L. Let $S = \{\alpha_i\}_{i\in I}$, $T = \{\beta_j\}_{j\in J}$ be F-bases for K_1 and K_2. Then $R = \mathrm{Span}_F\{\alpha_i\beta_j\}_{(i,j)\in I\times J}$ is a subring R of L.*

R contains 0, 1 and is closed under addition. We show it's closed under multiplication.

Consider elements x, $y \in R$, so that

$$x = \sum_{i\in I, j\in J} c_{ij}\alpha_i\beta_j, \quad y = \sum_{i\in I, j\in J} d_{ij}\alpha_i\beta_j,$$

for some c_{ij}, $d_{ij} \in F$ (almost all zero). Since K_1 is closed under multiplication, and $\{\alpha_i\}_{i\in I}$ is an F-basis for K_1, for $i_1, i_2 \in I$, we have

$$\alpha_{i_1}\alpha_{i_2} = \sum_i a_i\alpha_i$$

for some $a_i \in F$. Similarly for j_1, $j_2 \in J$

$$\beta_{j_1}\beta_{j_2} = \sum_j b_j\beta_j$$

for some $b_j \in F$. Then

$$\alpha_{i_1}\alpha_{i_2}\beta_{j_1}\beta_{j_2} = \sum_{i,j} a_ib_j\alpha_i\beta_j \in V.$$

Since the product xy is a linear combination of elements of the form above, we have $xy \in R$. This shows R is a subring of L.

Corollary 3.10. *Suppose the assumptions are the same as in the proposition, that furthermore K_1, K_2 are algebraic over F. Then $K_1K_2 = R$.*

Proof. We have $R \subseteq K_1K_2$, since R is a linear combination of $\alpha_i\beta_j$. On the other hand $K_1, K_2 \subseteq R$. It's enough to show R is a field, since then $K_1K_2 \subseteq R$.

Since K_1/F, K_2/F are algebraic extensions, α_i, β_j are algebraic over F. By Corollary 3.5, so are $\alpha_i\beta_j$ and $\sum_{i,j} c_{ij}\alpha_i\beta_j$, $c_{ij} \in F$. This shows every element of R is algebraic over F.

Let $\gamma \in R$ be non-zero. Since γ is algebraic over F, $F(\gamma)$ is the image of $F[X] \to L$, $p(X) \to p(\gamma)$. Since $p(\gamma) \in R$ for each $p(X) \in F[X]$, we have $F(\gamma) \subset R$. Since $F(\gamma)$ is a field, $\gamma^{-1} \in R$. This shows R is a field, and that $R = K_1K_2$. □

Corollary 3.11. *Suppose K_1, K_2 are algebraic extensions of F, inside a bigger extension L. Then $[K_1K_2 : K_2] \leq [K_1 : F]$.*

Proof. By the previous corollary, K_1K_2 is spanned by $\{\alpha_i\beta_j\}$, where $\{\alpha_i\}_{i\in I}$, $\{\beta_j\}_{j\in J}$ are F-bases for K_1 and K_2. Then we can write each element of K_1K_2 as

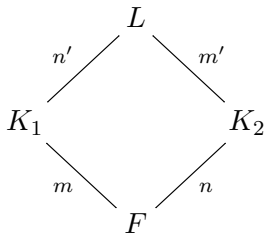
$$\sum_{i,j} c_{ij}\alpha_i\beta_j = \sum_{i\in I}\left(\sum_{j\in J} c_{ij}\beta_j\right)\alpha_i, \quad c_{ij} \in F.$$

Since $\sum_j c_{ij}\beta_j \in K_2$, this shows K_1K_2 is spanned by $\{\alpha_i\}$ over F. □

Let K_1/F and K_2/F be finite extensions of F, contained in L. By the corollary, and Theorem 3.1 we have

$$[K_1K_2 : F] = [K_1K_2 : K_2][K_2 : F] \leq [K_1 : F][K_2 : F].$$

Consider the diagram of field extensions

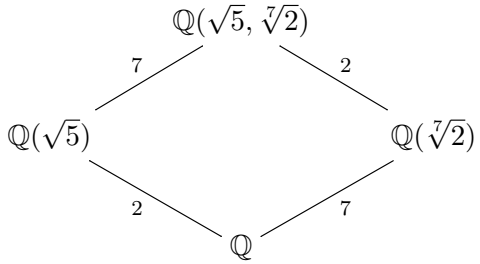


where labels indicate the degree of the extension. We have

$$mn' = [L : K_1][K_1 : F] = [L : F] = [L : K_2][K_2 : F] = m'n.$$

Suppose that $\gcd(m, n) = 1$. Then $m|m'n$ implies $m|m'$. On the other hand, by the corollary above $m' \leq m$. Then necessarily $m = m'$, and similarly $n = n'$.

Example We have a diagram of extensions



We know that $\sqrt[7]{2}$ is a root of X^7-2, which is irreducible over $\mathbb{Q}$. On the other hand, $[Q(\sqrt{5}, \sqrt[7]{2}) : \mathbb{Q}(\sqrt{5})] = 7$ is the degree of the minimal polynomial of $\sqrt[7]{2}$ over $\mathbb{Q}(\sqrt{5})$. Then $X^7 - 2$ must be this minimal polynomial. In particular $X^7 - 2$ is irreducible over $\mathbb{Q}(\sqrt{5})$.

4. Lecture 4: Straightedge and Compass Constructions

The mathematical tradition of the West goes back to the ancient Greeks, for whom mathematics was largely geometry, and a number was more or less the length of a line segment. The followers of Pythagoras were said to have been scandalized when they realized the hypotenuse of an isosceles right-angled triangle is not *commensurable* with its other sides, meaning no multiple of it is a multiple of those sides. Nowadays we interpret that as $\sqrt{2}$ being just one of uncountably many irrational numbers, whose existence we take for granted. But for the ancient Greeks the evidence for the existence of an irrational number was a geometric construction of a line segment having that length.

There were several infamous problems in the ancient world whose solution appeared impossibly difficult. Three of these are:

(1) Squaring the circle: Given a circle, construct a square that has the same area.
(2) Doubling the cube: Given a cube, construct another cube with twice the volume.
(3) Trisecting an angle: Given an angle, divide it into three equal parts.

The construction was to be done using only a *straight-edge* and *compass*, the principal tools of geometry to the ancient Greeks. A straight-edge is a ruler without markings. It took over two-thousand years, and the development of modern algebra, to finally prove these constructions were impossible.

With a straight-edge and compass one may only:

(1) draw a straight line,
(2) draw a circle.

It follows that the only *points* one can construct with a straight-edge and compass are at:

(1) the intersection of two lines,
(2) the intersection of two circles,
(3) the intersection of a line and a circle.

Let S be a set of points on the plane. For $P_1, P_2 \in S$, $P_1 \neq P_2$, let

$$\begin{aligned} P_1P_2 = &\text{ line passing through } P_1 \text{ and } P_2. \\ C(P_1, P_2) = &\text{ circle centered at } P_1 \text{ and passing through } P_2. \end{aligned}$$

From S we may construct a new point Q by either

(1) Taking P_1, P_2, Q_1, $Q_2 \in S$, and marking $Q \in P_1P_2 \cap Q_1Q_2$.
(2) Taking $P_1, P_2, O, P \in S$, and marking $Q \in P_1P_2 \cap C(O, P)$.
(3) Taking $O, O', P, P' \in S$, and marking $Q \in C(O, P) \cap C(O', P')$.

Definition 4.1. A point P is called *directly constructible* from S if it's the marked point obtained by one of the above constructions. A point P is called *constructible* from S if there exists a sequence of sets

$$S = S_0 \subset S_1 \subset S_2 \cdots \subset S_n,$$

where each $S_i = S_{i-1} \cup \{P_i\}$, for a point P_i directly constructible from S_{i-1}, and $P = P_n$. A length ℓ constructible from S is the distance between two points P, Q, each constructible from S.

Now let us apply algebraic geometry to the question of constructibility, a tool that was not available to the ancient Greeks. We consider all points as elements of $\mathbb{R}^2$, identifying them with their coordinates (x, y). We pick a point $O \in S$ and identify it as the origin $(0, 0)$. We also pick distinct points $P_0, Q_0 \in S$ and identify $|P_0Q_0|$ with the unit length, i.e. 1.

Proposition 4.2. *A length ℓ is constructible from S if and only if the point $(0, \ell)$ is constructible.*

Proof. If the point $(0, \ell)$ is constructible, its distance from $(0, 0)$ is ℓ, so ℓ is a constructible length.

Now assume the line segment PQ has length ℓ, with $P, Q \in S$.

Suppose PQ does not pass through O. Draw the line parallel to OP and passing through Q, as well as the line parallel to PQ passing through O. Let R denote the intersection. Then $OPQR$ is a parallelogram, and OR has length PQ. Draw a circle with center O passing through R. It will intersect the x-axis at the point $(0, \ell)$.

If O is one of P and Q then the last step above again constructs $(0, \ell)$.

Suppose now that P,Q,O are three distinct points lying on the same line L. Draw the lines $L1$ and $L2$ perpendicular to L passing through Q and O. Using the compass, mark the point P' on $L1$, so that $|OP'| = |OP|$. Draw the line parallel to PQ passing through P' and let it intersect $L2$ at Q'. Now $PQQ'P$ is a rectangle and $|QQ'| = |OP'| = |OP|$. Draw the circle at Q with radius QQ'

and let it intersect L at R. Then $|OR| = |PQ|$. The circle at O passing through R intersects the x-axis at $(\ell, 0)$. □

Thus the question of constructible length is equivalent to the question of constructing points (x, y) with certain coordinates, which may be investigated with algebraic geometry.

Suppose two points with coordinates (x_0, y_0) and (x_1, y_1) are given. The line through these points has equation

$$Ax + By + C = 0$$

where

$$A = y_0 - y_1, \quad B = x_1 - x_0, \quad C = x_0y_1 - x_1y_0.$$

Note that the coefficients are *polynomials* in the coordinates of the given points.

The intersection of two lines

$$Ax + By + C = 0, \quad A'x + B'y + C' = 0$$

is non-empty if and only if $AB' - A'B \neq 0$, in which case the intersection point is

$$x_0 = \frac{BC - B'C'}{AB' - A'B}, \quad y_0 = \frac{A'C' - AC}{AB' - A'B}.$$

The coordinates of the intersection point are *rational functions* in the coefficients of the given equations. It follows that

Proposition 4.3. *Let S be a set of points whose coordinates lie in a field $F \subset \mathbb{R}$. If a point P is directly constructed from S by intersecting two lines, then P will also have coordinates in F.*

Given two points (x_0, y_0) and (x_1, y_1), the line segment connecting them has length

$$\sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2}.$$

Using a compass, one may draw a circle with center at a given point (a, b), that passes through another point (x_0, y_0). The equation of such a circle is

$$(x - x_0)^2 + (y - y_0)^2 = (x_0 - a)^2 + (y_0 - b)^2.$$

Note the coefficients of this equation are again polynomials in a, b, x_0, y_0.

Suppose we have a line and a circle given by equations

$$Ax + By + C = 0, \quad (x - x_0)^2 + (y - y_0)^2 = S.$$

To find the coordinates of the intersection point (x, y) one will have to solve a quadratic equation. The formula for, say x, will look like

$$ax^2 + bx + c = 0$$

where a, b, c are quantities that may be expressed as polynomials in A, B, C, x_0, y_0. Suppose the latter lie in a field F. The quadratic formula

$$x = \frac{-b \pm \sqrt{\Delta}}{2a}, \quad \Delta = b^2 - 4ac$$

will then imply that x lies in a *quadratic extension* of F, namely $F(\sqrt{\Delta})$. Since y is a rational function of x, it also belongs to $F(\sqrt{\Delta})$. We have therefore shown:

Proposition 4.4. *Let $S \subset \mathbb{R}^2$ be a set of points whose coordinates lie in F. If a point Q is directly constructed from S by intersecting $C(O, P)$ with P_1P_2, $O, P, P_1, P_2 \in S$, then the coordinates of Q lie in a quadratic extension of F.*

Suppose we have two circles

$$(x-x_0)^2+(y-y_0)^2=q_0,\quad (x-x_1)^2+(y-y_1)^2=q_1.$$

If we expand and subtract one equation from the other, we obtain the equation of a line, since the x^2 and y^2 terms will cancel out. It has the form

$$Ax+By+C=0$$

where

$$A=2x(x_1-x_0),\quad B=2y(y_1-y_0),\quad C=x_0^2-x_1^2+y_0^2-y_1^2-q_0+q_1.$$

Then intersecting the two circles is the same as intersecting either of them with the line above. Note that the coefficients A, B, C are again polynomials in x_0, y_0, x_1, y_1, q_0 and q_1.

We have therefore shown:

Proposition 4.5. *Suppose $S\subset\mathbb{R}^2$ has points with coordinatess in a field F. Then a point P is directly constructible from S only if P has coordinates in a quadratic extension $F(\sqrt{D})$.*

Conversely, suppose D is the length of a line segment PQ with $P,Q\in F$. Draw a circle with unit length centered at Q and let it intersect PQ at Q', such that $|PQ'|=D+1$. Mark the midpoint of PQ as O and draw the circle C centered at O passing through P. Draw also the line perpendicular to QQ' and passing through Q. If X is one of the two intersection points of this line with C, then $|XQ|=\sqrt{D}$.

Theorem 4.6. *Let S be a finite set of points containing the origin and two points P, Q with $|PQ|=1$. Let F denote the field generated over $\mathbb{Q}$ by the coordinates of the points in S. A length ℓ is constructible from S if and only if there exists a sequence*

$$F_0=F\subset F_1\subset F_2\subset\cdots\subset F_n,$$

where each F_i is a quadratic extension of F_{i-1}, and $\ell\in F_n$.

Corollary 4.7. *Let S and F be as in the theorem. If a length $\ell\in\mathbb{R}$ is constructible, then it is algebraic over F of degree 2^k for some k.*

Proof. We have $[F_n:F_0]=2^n$. If $K=F(\ell)$, then ℓ has degree $[K:\mathbb{Q}]$ which divides $[F_n:F]=2^n$, and so must be 2^k for some k. □

Corollary 4.8. *It is impossible to square the circle, double the cube, or trisect an angle in general.*

Proof. Let C be a given circle passing through O and P. Let $S=\{O,P\}$, take the line OP to be the x-axis and $|OP|$ to have unit length. The field generated by the coordinates of P and O is $\mathbb{Q}$. To construct a square is equivalent to constructing its side length. The circle C has area π, so a square with that area has side length $\sqrt{\pi}$. But $\sqrt{\pi}$ is not algebraic over $\mathbb{Q}$, and in particular does not have degree 2^k over $\mathbb{Q}$.

To construct a cube whose area is double that of the unit cube is to construct a length ℓ such that $\ell^3=2$, but $\ell=\sqrt[3]{2}$ has degree 3 over $\mathbb{Q}$.

To construct an angle θ is equivalent to constructing the point $(\cos\theta,\sin\theta)$. Consider the triple angle formula

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

Let $\theta=20^\circ$. Then $\ell=2\cos(\theta)$ satisfies

$$\frac{1}{2}=4(\ell/2)^3-3\ell/2\iff\ell^3-3\ell-1=0.$$

The line making angle $3\theta=60^\circ$ with the x-axis passes through $(1,\sqrt{3})$. In particular, 60° is a constructible angle. But the polynomial X^3-3X-1 is irreducible over $\mathbb{Q}$, so ℓ has degree 3 over $\mathbb{Q}$, and is not constructible. □

5. Splitting Fields

Let F be a field, and $f[x] \in F[x]$ a polynomial. We want to define *the* smallest extension of F containing all the roots of $f[x]$, in some appropriate sense. It will turn out such extensions always exist and are unique up to isomorphism.

Proposition 5.1. *Let F be a field, and $f[x] \in F[x]$ a polynomial. There exists a finite extension L/F, of degree at most $\deg(f)!$, such that $f[x]$ factors completely over L.*

Proof. We proceed by induction on $n = \deg(f)$. If $n \leq 1$ this is trivial, since then $f[x]$ already factors completely over F.

Assume the result is true for all polynomials of degree $< n$. Let $f_1(x)$ be an irreducible factor of $f(x)$ over F, and put $F_1 = F[x]/(f_1(x))$. Then $f_1(x)$ has a root $\alpha \in F_1$, $F_1 = F(\alpha)$ and $[F_1 : F] = \deg f_1$. For some $g(x) \in F_1[x]$ of degree $n-1$, we have $f(x) = (x-\alpha)g(x)$. By the induction hypothesis, there exists some extension K/F_1, of degree at most $(n-1)!$ such that $g(x)$ splits completely over K, hence so does $f(x)$. Since $[F_1 : F] = \deg f_1 \leq \deg f = n$, $[L : F] = [L : F_1][F_1 : F] \leq (n-1)!n = n!$, which shows the extension L/F is as claimed.

By induction, all $f[x] \in F[x]$ split over a field L/F of degree at most $\deg(f)!$. □

Example 5.2. Consider $x^3 - 2$ over $\mathbb{Q}$. We can identify $F_1 = \mathbb{Q}[x]/(x^3-2)$ with $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{C}$ over which

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}).$$

Then $F_2 = \mathbb{Q}(\sqrt[3]{2})[x]/(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$ has degree $3 \cdot 2 = 6$ over $\mathbb{Q}$, and may be identified with

$$\mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) \subset \mathbb{C},$$

where $\zeta_3 = e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2}$, and

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \zeta_3\sqrt[3]{2})(x - \zeta_3^2\sqrt[3]{2}).$$

It may happen that $f(x)$ splits completely over an extension of degree strictly smaller than $\deg(f)!$, as the following example shows.

Example 5.3. Consider $f(x) = x^3 - 2 \in \mathbb{F}_7[x]$. Modulo 7 the only cubic residues are ± 1, so $f(x)$ has no root in $\mathbb{F}_7$, hence is irreducible. Let $K = \mathbb{F}_7[x]/(x^3-2)$, which we may write as $\mathbb{F}_7(\alpha)$ for $\alpha^3 = 2$. Now note that $\{2, 4, 1\} \subset \mathbb{F}_7^\times$ are third roots of unity, hence $f(2\alpha) = f(4\alpha) = 1$. Then

$$x^3 - 2 = (x-\alpha)(x-2\alpha)(x-4\alpha) \in K[x]$$

so that $x^3 - 2$ factors completely over an extension of $\mathbb{F}_7$ of degree $3 < 6$.

Given a polynomial in $F[x]$, we would like to identify a certain *minimal* field extension K/F over which it splits.

Definition 5.4. A *splitting field* of $f[x] \in F[X]$ over F is an extension K/F such that:

(i) $f[x]$ factors completely over K.
(ii) $f[x]$ does not factor completely over a proper subfield of K.

Proposition 5.5. *Any polynomial $f[x] \in F[x]$ has a splitting field K/F.*

Proof. By Proposition 5.1, there exists a finite extension L/F in which $f(x)$ factors completely. Let $\alpha_1, \cdots, \alpha_n \in L$ be the roots of $f(x)$. If $K \subset L$ is a subfield of L containing F, then $f(x)$ splits over K if and only if K contains the roots α_i. The field $F(\alpha_1, \cdots, \alpha_n)$ is minimal with respect to this property, hence it is a splitting field of $f(x)$. □

Splitting field have a uniqueness property that allows us to speak of *the* splitting field of a polynomial.

Proposition 5.6. *Let $f(x) \in F[x]$, $\varphi : F \to F'$ a field isomorphism, and $g(x) \in F'[x]$ the polynomial obtained by applying φ to the coefficients of f. Suppose that K/F is a splitting field for $f(x)$, and K'/F' a splitting field for $g(x)$. Then φ extends to an isomorphism $\varphi' : K \to K'$.*

Proof. We prove this by induction on the degree n of f. If $n = 1$, then $f(x) = x - \alpha$ for some $\alpha \in F$, $g(x) = x - \varphi(\alpha)$. Then F is the splitting field of $f(x)$ and F' the splitting field of $g(x)$, and φ is an isomorphism of the two trivially extending itself.

Suppose now the result is true for polynomials of degree $< n$. Let $\alpha_1 \in K$ be a root of $f(x)$, and $f_1(x) \in F[x]$ an irreducible factor of $f(x)$ such that $f_1(\alpha) = 0$. Put $F_1 = F(\alpha_1)$. Let $g_1(x)$ be the obtained from $f_1(x)$ by applying φ_1 to the coefficients. Then $g_1(x)$ is irreducible over F' since $f_1(x)$ is over F. Let $\beta_1 \in K'$ be a root of $g_1(x)$, and put $F_1' = F'(\beta)$. By Theorem 2.2, the isomorphism $\varphi : F \to F'$ extends to an isomorphism $\varphi_1 : F_1 \to F_1'$. Write $f(x) = f_1(x)f_0(x)$ and $g(x) = g_1(x)g_0(x)$. Then $g_1 \in F_1'[x]$ is φ_1 applied to the coefficients of $f_0(x) \in F_1[x]$.

Let $\alpha_1, \cdots, \alpha_n$ be all the roots of $f(x)$. Since K/F is a splitting field, the subfield $F(\alpha_1, \cdots, \alpha_n) \subseteq K$ is equal to K itself. Likewise, if $\beta_1, \cdots, \beta_n$ are the roots of $g(x)$ in K', then $F'(\beta_1, \cdots, \beta_n) \subseteq K'$ is K' itself. Then $K = F_1(\alpha_2, \cdots, \alpha_n)$, and $K' = F_1'(\beta_2, \cdots, \beta_n)$. Since $\alpha_2, \cdots, \alpha_n$ are the roots of $f_0(x)$, K is the splitting field of $f_0(x)$ over F_1. Likewise K' is the splitting field of $g_0(x)$ over F_1'. As $\deg f_0(x) < n$, by the induction hypothesis the isomorphism $\varphi_1 : F_1 \to F_1'$ extends to an isomorphism $K \to K'$.

Therefore by induction the proposition holds for $f(x)$ of all degrees. □

Corollary 5.7. *Let K/F and K'/F be two splitting fields for $f(x) \in F[x]$. Then there exists an F-linear isomorphism $K \to K'$.*

Proof. This follows from the proposition applied to $\varphi = \mathrm{id} : F \to F$. □

We have seen that the process of adjoining all roots of a polynomial $f(x) \in F[x]$ to F, gives a well-defined field extension that is unique up to isomorphism. Next we consider what happens if we adjoin all roots of *all* polynomials in $F[x]$.

Definition 5.8. Let F be a field. An algebraic extension L/F is called an *algebraic closure* of F, if every polynomial $f(x) \in F[x]$ splits completely over L.

Definition 5.9. A field K is called *algebraically closed* if every polynomial $f(x) \in K[x]$ splits completely over K.

The most well-known example of an algebraically closed field is $\mathbb{C}$. Let us for the moment take this fact for granted. Note that although every polynomial $f(x) \in \mathbb{Q}[x]$ splits completely over $\mathbb{C}$, $\mathbb{C}$ is not an algebraic closure of $\mathbb{Q}$, since it is not an algebraic extension. However, the subfield of $\mathbb{C}$ generated over $\mathbb{Q}$ by all the roots of all polynomials $f(x) \in F[x]$ is an algebraic closure of $\mathbb{Q}$, denoted $\overline{\mathbb{Q}}$. It is in fact algebraically closed.

Proposition 5.10. *Let K/F be an algebraic closure of F. Then K is algebraically closed.*

Proof. Let $f(x) \in K[x]$, and suppose α is a root of f in $K(\alpha)$. Then α is algebraic over K, and K is algebraic over F, hence α is algebraic over F. Therefore there exists a polynomial $g(x) \in F[x]$, such that $g(\alpha) = 0$. As K is an algebraic closure of F, $g(x)$ splits completely over K, and so $\alpha \in K$. Then all roots of $f(x)$ belong to K and so $f(x)$ splits over it. □

To show algebraic closures exist, we first show there exists an algebraically closed extension of a given field.

Proposition 5.11. *Let F be a field. Then there exists an algebraically closed field L containing F.*

Proof. First we adjoin to F an infinite number of variables x_f, one for each $f \in F[x]$. Let $R = F[\cdots, x_f, \cdots]$ be the corresponding polynomial ring over F with infinitely many variables. Let $I \subset R$ be the ideal generated by $f(x_f)$ for all $f \in F[x]$.

First we claim I is a proper ideal of R. Otherwise, there exist polynomials $f_1(x_{f_i}), \cdots, f_n(x_{f_n})$, and $g_1, \cdots, g_n \in R$ such that

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

Let $x_i = x_{f_i}$, for $i = 1, \cdots, n$. Extend the list to $x_1, \cdots, x_m$ such that it contains all variables occuring in g_i. There exists an extension F'/F in which each $f_i(x)$ has a root α_i. Set $x_i = \alpha_i$ for $i \leq n$, and $x_i = 0$ for $i > n$. Then the equation above says $0 = 1$ in F', which is impossible. Hence, I is a proper ideal of R.

Let $\mathfrak{m} \subset R$ be a maximal ideal containing I. Then $K_0 = F_0/\mathfrak{m}$ is a field, which contains F. But since $f(x_f) \in \mathfrak{m}$, the image of x_f in K_0 is a root of $f(x) \in F[x]$. Therefore all polynomials $f(x) \in F[x]$ have a root in K.

Now apply this construction again to K_0, and obtain K_1/K_0 in which all polynomials $f(x) \in K[x]$ have a root. Then apply it again to K_1 and obtain K_2, and so on K_3, K_4, etc. Put

$$K = \cup_i K_i$$

. Then K is a field containing all K_i. If $f(x) \in K[x]$, it lies in $K_i[x]$ for some $K_i \subset K$, so it has a root in K_{i+1}. Thus every such $f \in K[x]$ has a root in K. It follows that f splits completely in K, hence K is algebraically closed. □

Given a field F, let K/F be an algebraically closed extension, and denote by $\overline{F}/F$ the subfield of all $\alpha \in K$ which are algebraic over F.

Proposition 5.12. *$\overline{F}/F$ is an algebraic closure of F, and any other algebraic closure is isomorphic to F.*

Proof. Let $f(x) \in F[x]$. Then $f(x) = \prod_i (x - \alpha_i)$ for $\alpha_i \in K$. In particular, α_i are algebraic over F, hence belong to $\overline{F}$. Therefore $f(x)$ splits over $\overline{F}$. □

6. Separability

Let F be a field of characteristic $p > 0$. Consider the function

$$\phi : F \to F, \quad \phi(x) = x^p.$$

Proposition 6.1. *The map ϕ is a field homomorphism.*

Proof. It's clear that $\phi(1) = 1$ and $\phi(xy) = \phi(x)\phi(y)$. We have

$$\phi(x+y) = (x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \binom{p}{2} x^{p-2} y^2 + \cdots + \binom{p}{1} x y^{p-1} + y^p.$$

Note that if $0 < k < p$, the numerator of

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

is divisible by p, but not its denominator. Since $\binom{p}{k}$ is an integer, it must be a multiple of p, hence equal to 0 in F. Therefore

$$\phi(x+y) = x^p + y^p = \phi(x) + \phi(y).$$

□

Definition 6.2. The map $\phi : F \to F$ is called the *Frobenius* homomorphism.

Corollary 6.3. *If F is a finite field of characteristic $p > 0$, the Frobenius is bijective.*

Proof. An injective function from a finite set to itself is surjective. □

Let $F = \mathbb{F}_p(t)$. It is an infinite field of characteristic p. Consider the polynomial

$$f(x) = x^p - t \in F[x].$$

Let K/F be a splitting field for $f(x)$, and $\alpha \in K$ a root of $f(x)$. Then we have

$$f(x) = x^p - \alpha^p = (x - \alpha)^p.$$

Then all the roots of $f(x)$ in K are *equal*. If $m_\alpha(x)$ is the minimal polynomial of $f(x)$ over F, it must equal $(x-\alpha)^k$. If $p = kq + r$, $0 \leq r < p$, then

$$f(x) = m_\alpha(x)^q \cdot (x - \alpha)^r,$$

so that $(x-\alpha)^r \in F[x]$. Since $(x-\alpha)^k$ is the minimal polynomial, and $r < k$, r must be zero.

It follows that $x^p - t$ is *irreducible* over $\mathbb{F}_p(t)$, and yet all its roots (in the splitting field) are equal. When we study Galois theory, we will want to study the splitting field of the polynomial by the symmetries of its roots. But in this example, there are no symmetries to investigate, because there's only a single root. This forces us to make careful distinctions between general splitting fields.

Definition 6.4. A polynomial $p(x)$ over a field F is called *separable* if its roots are distinct (in the splitting field). Otherwise it's called *inseparable*.

Fortunately, it's not usually necessary to calculate the splitting field of $p(x)$ in order to tell whether it's separable or not.

Note that over any field, a polynomial

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

has a well-defined derivative

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

Proposition 6.5. *A polynomial $p(x) \in F[x]$ is separable if and only if $p(x)$ and $p'(x)$ have no common root.*

Proof. Let

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

be the factorization of $p(x)$ over the splitting field. By the Leibniz formula for differentiation

$$p'(x) = c\left(\frac{p(x)}{x-\alpha_1} + \frac{p(x)}{x-\alpha_2} + \cdots \frac{p(x)}{x-\alpha_n}\right).$$

Note each term in the sum is actually a polynomial. If $p(x)$ is inseparable, $\alpha_i = \alpha_j$ for some $i \neq j$. Then α_i is a root of $p(x)/(x-\alpha_k)$ for all k, hence $p'(\alpha_i) = 0$, and α_i is a common root of $p(x)$ and $p'9x)$.

Conversely, if $\alpha_i - \alpha_j \neq 0$ for $i \neq j$, then

$$p'(\alpha_i) = c\prod_{i \neq j}(\alpha_i - \alpha_j) \neq 0,$$

so that α_i is not a root of $p'(x)$. □

Note that $p(x), q(x) \in F[x]$ have no common root if and only if $\gcd(p(x), q(x)) = 1$, a condition that can be checked in $F[x]$ using the Euclidean algorithm, without needing to compute any field extensions.

Example 6.6. For $p(x) = x^p - t \in \mathbb{F}_p(t)$ we have

$$p'(x) = px^{p-1} = 0.$$

Then $\gcd(p(x), p'(x)) = p(x) \neq 1$.

Corollary 6.7. *An irreducible $p(x) \in F[x]$ is separable if and only if $p'(x) \neq 0$.*

Proof. If $p'(x) = 0$, then $p(x)|p'(x)$ and $p(x)$ is inseparable by the proposition.

Suppose $p'(x) \neq 0$. Then

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

where $\deg(r) < \deg(p')$. If $p(x)$ has a double root α, $r(\alpha) = p(\alpha) - p'(\alpha)q(\alpha) = 0$. Then $m_\alpha(x)|r(x)$, so that $m_\alpha(x) \neq p(x)$, and $p(x)$ is reducible. □

Corollary 6.8. *If F has characteristic zero, every irreducible $p(x) \in F[x]$ is separable.*

Corollary 6.9. *If F has characteristic $p > 0$ and $p(x) = a_n x^n + \cdots + a_1 x + a_0$ is inseparable, then $p|k$ for each non-zero a_k.*

Proof. The coefficients of $p'(x)$ are ka_k. If $p(x)$ is irreducible and inseparable so

$$p'(x) = 0 \Longrightarrow ka_k = 0 \ \forall k \implies p|k \text{ if } a_k \neq 0.$$

□

Definition 6.10. A field F is called *perfect* if every irreducible $p(x) \in F[x]$ is separable.

Definition 6.11. A field extension K/F is called *separable*, if $m_\alpha(x)$ is separable for all $\alpha \in K$.

Therefore the fields of characteristic zero, such as $\mathbb{Q}$, $\mathbb{C}$, or $\mathbb{Q}(\sqrt{2})$ are all perfect, and all their finite extensions are separable.

Proposition 6.12. *If F has characteristic $p > 0$, the following are equivalent:*

1. *F is perfect.*
2. *The Frobenius $\phi(x) = x^p$ is surjective.*
3. *Every finite extension of F is separable.*

Proof. (1) $\Longrightarrow$ (2) : Suppose F is perfect, and $a \in F$. Let K/F be the splitting field of $x^p - a$, and $\beta \in K$ such that $\beta^p = a$. Then the characteristic polynomial $m_\beta(x)$ over F is irreducible, and divides $x^p - a = x^p - \beta^p = (x - \beta)^p$. Since F is perfect, m_β has no repeated root, so $m_\beta = x - \beta$, and $\beta \in F$.

(2) $\Longrightarrow$ (3) : Let K/F be a finite extension, and $\alpha \in K$, $m_\alpha(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Assume $m_\alpha(x)$ is inseparable, so that $m'_\alpha(x) = 0$ and $p|k$ whenever $a_k \neq 0$, by Corollary 6.9. Since ϕ is surjective, each $a_k = b_k^p$ for some $b_k \in F$. Then

$$m_\alpha(x) = (b_m x^m)^p + (b_{m-1}x^{m-1})^{p-1} + \cdots + (b_1 x)^p + b_0^p = q(x)^p$$

where

$$q(x) = b_m x^m + \cdots + b_1 x + b_0$$

which contradicts irreducibility of $m_\alpha(x)$. Therefore $m_\alpha(x)$ must be separable.

(3) $\Longrightarrow$ (1) : Suppose $p(x) \in F[x]$ is irreducible. Then $K = F[x]/(p(x))$ is a separable extension of F. If $\alpha \in K$ is the image of $x \in F[x]$, then $m_\alpha(x) = p(x)$ is separable. □

Corollary 6.13. *Finite fields are perfect.*

7. Finite and cyclotomic fields

Let $n > 1$, and suppose $K/\mathbb{F}_p$ is a finite extension of degree n. Then K is a finite field with p^n elements. The group $K^\times$ has $p^n - 1$ elements, and so for all $a \in K^\times$, $a^{p^n - 1} = 1$. Then every $a \in K$ is a root of $x^{p^n} - x$. On the other hand, $x^{p^n} - x \in \mathbb{F}_p[x]$ has degree p^n, so K is exactly the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.

Conversely, for each $n > 1$, $p(x) = x^{p^n} - x$ is separable, since $p'(x) = -1 \neq 0$. Then $p(x)$ has p^n roots in its splitting field K. Let $S \subset K$ be the set of roots of $p(x)$. For $\alpha, \beta \in S$ we have

$$p(\alpha + \beta) = (\alpha + \beta)^{p^n} - (\alpha + \beta) = \alpha^{p^n} - \alpha + \beta^{p^n} - \beta = p(\alpha) + p(\beta) = 0$$

$$p(\alpha \cdot \beta) = (\alpha\beta)^{p^n} - \alpha\beta = \alpha^{p^n}\beta^{p^n} - \alpha\beta = \alpha\beta - \alpha\beta = 0.$$

$$p(1) = p(0) = 0.$$

It follows that S is a *subfield* of K. But K is the smallest field extension of F containing S, so $S = K$. Then K has p^n elements, and therefore has degree n over K.

We have shown that

Proposition 7.1. *$\mathbb{F}_p$ has a unique extension of degree n, equal to the splitting field of $x^{p^n} - x$.*

This unique extension is denoted $\mathbb{F}_{p^n}$. The proposition shows that $\mathbb{F}_{p^n}$ are exactly all the finite fields of characteristic p. They form a tower of extensions

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^3} \cdots .$$

If $p(x)$ is any polynomial over $\mathbb{F}_p$, it's splitting field must be $\mathbb{F}_{p^n}$ for some n.

If p is an irreducible polynomial of degree n, then $\mathbb{F}_p[x]/(p(x))$ is a degree n extension of $\mathbb{F}_p$, and hence isomorphic to $\mathbb{F}_{p^n}$. It follows that every irreducible polynomial over $\mathbb{F}_p$ of degree n has a root in $\mathbb{F}_{p^n}$.

Recall the Frobenius map $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n},\ \phi(x) = x^p$, which is a field automorphism of $\mathbb{F}_{p^n}$.

Definition 7.2. The group of all nth roots of unity is denoted μ_n.

Since each such root is $e^{2\pi ik/n}$ for some $k = 0, \cdots, n-1$, μ_n is cyclic, and isomorphic to $\mathbb{Z}/n\mathbb{Z}$. The *primitive nth roots of unity* are the elements $\zeta \in \mu_n$ that generate the entire group.

We know that $x^n - 1$ is separable (has no repeated roots), since

$$x^n - 1 = \sum_{\zeta \in \mu_n} (x - \zeta).$$

In fact, the same is true over $\mathbb{F}_p$.

Definition 7.3. The nth cyclotomic polynomial is

$$\Phi_n(x) = \sum_{\text{primitive } \zeta \in \mu_n} (x - \zeta).$$

If $n = p$ is prime, all the non-identity roots of $x^p - 1$ are primitive, so that

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

In general, $\Phi_n(x)$ has degree $\phi(n)$.

Let $\zeta \in \mu_n$ be an element of order d. Then $d|n$ and ζ is a primitive dth root of unity. Conversely, any primitive dth root of unity such that $d|n$ belongs to μ_n, since $\zeta^n = (\zeta^d)^e = 1$ for $n = de$. Then

$$x^n - 1 = \sum_{\zeta \in \mu_n} (x - \zeta) = \prod_{d|n} \prod_{\text{primitive } \zeta \in \mu_d} (x - \zeta) = \prod_{d|n} \Phi_d(x).$$

This allows us to compute Φ_n for non-prime n inductively. For instance

$$x^4 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x) = (x-1)(x+1)\Phi_4(x) \Longrightarrow \Phi_4(x) = x^2 + 1,$$
$$x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) = (x-1)(x+1)(x^2+x+1)\Phi_6(x) \Longrightarrow \Phi_6(x) = x^2 - x + 1$$
$$x^8 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x) = (x^4-1)\Phi_8(x) \Longrightarrow \Phi_8(x) = x^4 + 1.$$
$$x^9 - 1 = \Phi_1(x)\Phi_3(x)\Phi_9(x) = (x-1)(x^2+x+1)\Phi_9(x) \Longrightarrow \Phi_9(x) = x^6 + x^3 + 1$$

The first few non-prime cyclotomic polynomials are then

$$\Phi_4(x) = x^2 + 1$$
$$\Phi_6(x) = x^2 - x + 1$$
$$\Phi_8(x) = x^4 + 1$$
$$\Phi_9(x) = x^6 + x^3 + 1.$$

It's *not* true that all coefficients of cyclotomic polynomials are 0, 1, or -1. The first counterexample is $n = 105$, which has two terms with coefficient -2. In fact the coefficients can be arbitrarily large. It *is* however a non-trivial fact that:

Theorem 7.4. *For each n, $\Phi_n(x)$ is a monic irreducible polynomial in $\mathbb{Z}[x]$.*

Proof. It's clear that $\Phi_n(x)$ is monic. We first prove it has integral coefficients by induction. It's true for $n = 1$ since $\Phi_1(x) = x - 1$. For $n > 1$ we have

$$x^n - 1 = f(x)\Phi_n(x)$$

where

$$f(x) = \prod_{d<n} \Phi_d(x)$$

is in $\mathbb{Z}[x]$ by induction. In particular, $f(x) \in \mathbb{Q}[x]$, and divides $x^n - 1 \in \mathbb{Q}[x]$, hence the quotient $\Phi_n[x]$ is also in $\mathbb{Q}[x]$. Note that by the division algorithm, quotients and remainders in polynomial rings are invariant under extension of scalar fields. Now $x^n - 1 = f(x)\Phi_n(x)$ is a factorization of $x^n - 1 \in \mathbb{Z}[x]$ over $\mathbb{Q}[x]$. Since $f(x)$ is monic and integral, by Gauss's lemma so is $\Phi_n(x)$.

Now we prove that $\Phi_n(x) \in \mathbb{Z}[x]$ is irreducible. Suppose $\Phi_n(x) = f(x)g(x)$ is a factorization, with $f(x)g(x) \in \mathbb{Z}[x]$, such that $f(x)$ is irreducible, and $f(\zeta) = 0$ for ζ a primitive nth root of unity.

Let p be a prime not dividing n. We have

$$g(\zeta^p) = 0 \iff \zeta \text{ a root of } g(x^p) \iff f(x)|g(x^p).$$

Let

$$\overline{\Phi}_n(x) = \overline{f}(x)\overline{g}(x)$$

be the corresponding factorization over $\mathbb{F}_p[x]$. If $f(x)|g(x^p)$ then $\overline{f}(x)|\overline{g}(x^p) = \overline{g}(x)^p$, and $\overline{f}(x)$ and $\overline{g}(x)$ must share a factor in common. But $\overline{\Phi}_n(x)$ divides $x^n - 1$, which has derivative $nx^{n-1} - 1$, which is non-zero in $\mathbb{F}_p[x]$. Then $x^n - 1 \in \mathbb{F}_p[x]$ is separable, so $\overline{f}(x)$ and $\overline{g}(x)$ have no factors in common. Therefore ζ^p is not a root of $g(x)$. Since it's a root of $\Phi_n(x)$, it must be a root of $f(x)$.

On the other hand, if a is any integer coprime to n, we can write $a = p_1 p_2 \cdots p_r$ where p_i are primes not dividing n. Then $\zeta^a = (((\zeta^{p_1})^{p_2})^{\cdots})^{p_r}$ is a root of $f(x)$. As any primitive nth root of unity is ζ^a for some a coprime to n, we obtain $\Phi_n(x)|f(x)$. In particular, $\Phi_n(x) = f(x)$ is irreducible. □

Corollary 7.5. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$

Note the proof is based on loosely two basic ideas. One idea is that one may compare the factorization of $x^n - 1$ over $\mathbb{Q}$ with that of $x^n - 1$ over $\mathbb{F}_p$, for $p \nmid n$. The second is to investigate how automorphisms of a finite field permute the roots of polynomials.

To expound on the second idea further, let us suppose $F(x)$ is a polynomial over $\mathbb{F}_p$, and $F(x) = f(x)g(x)$ for some $f(x)$, $g(x) \in \mathbb{F}_p[x]$. The splitting field of $F(x)$ is $\mathbb{F}_{p^n}$ for some n, and $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $\phi(x) = x^p$ is an automorphism. Since ϕ is the identity on $\mathbb{F}_p$, it must permute the roots of $F(x)$. Suppose α is a root of $f(x)$. Then $\phi(\alpha) = \alpha^p$ is a root of either $f(x)$ or $g(x)$. But $g(\alpha^p) = g(\alpha)^p$, so $g(\alpha^p) = 0$ implies $g(\alpha) = 0$. Then *assuming* that $F(x)$ is separable, the Frobenius permutes the roots of the different factors of $F(x)$ separately.

Studying how automorphisms of a splitting field of a polynomial act on the roots, naturally leads to Galois theory, which we study next.

8. Galois Theory

If K is a field, $\mathrm{Aut}(K)$, the set of field isomorphisms $\sigma : K \to K$ is a group under composition:

(i) Given $\sigma, \tau \in \mathrm{Aut}(K)$, the composition $\sigma \circ \tau$ is again in $\mathrm{Aut}(K)$, and this operation is associative.
(ii) For $\sigma \in \mathrm{Aut}(K)$, $\sigma \circ \mathrm{id} = \mathrm{id} \circ \sigma = \sigma$.
(iii) Each $\sigma : K \to K$ has an inverse $\sigma^{-1} : K \to K$.

Thus to each field K one may associative a group $\mathrm{Aut}(K)$.

Now suppose K/F is a field extension. To it we associate

$$\mathrm{Aut}_F(K) = \{\sigma \in \mathrm{Aut}(K) : \sigma(x) = x \text{ for all } x \in F\}.$$

It is a subgroup of $\mathrm{Aut}(K)$.

Suppose K_0 is the prime field of K, and $\sigma \in \mathrm{Aut}(K)$. Since $\sigma(1) = 1$, σ is the identity on the image of $\mathbb{Z} \to K_0$. Now either 1 generates K_0 as a group, or $K_0 = \mathbb{Q}$. Then for $a, b \in \mathbb{Z}$, $b \neq 0$, $\sigma(a/b) = \sigma(a)/\sigma(b) = a/b$. In either case $\sigma(x) = x$ for $x \in K_0$. This shows that $\mathrm{Aut}(K) = \mathrm{Aut}_{K_0}(K)$. Then $\mathrm{Aut}(K)$ is a special case of the group associated to an extension.

Let us fix some extension K/F, and let $G = \mathrm{Aut}_F(K)$. If L/F is a subextension of K, we obtain a subgroup $\mathrm{Aut}_L(K)$ of G. Indeed if $\sigma \in \mathrm{Aut}_L(K)$, then $\sigma(x) = x$ for all $x \in L$. In particular, $\sigma(x) = x$ for all $x \in F$, so $\sigma \in \mathrm{Aut}_F(K)$. Thus we obtain map

$$\{ \text{ subfields of } K \text{ containing } F \} \longrightarrow \{ \text{ subgroups of } \mathrm{Aut}_F(K) \}.$$

$$L/F \mapsto \mathrm{Aut}_F(L).$$

If $F \subset L_1 \subset L_2 \subset K$, then $\mathrm{Aut}_{L_2}(K) \subseteq \mathrm{Aut}_{L_1}(K)$. Thus the map above is inclusion reversing.

Now let $H \subset \mathrm{Aut}_F(K)$ be an arbitrary subgroup. Define

$$L_H = \{a \in K : \sigma(a) = a \text{ for all } \sigma \in H\}.$$

It's easy to check that L_H is a subfield of K containing F. Then we have obtained a map

$$\{ \text{ subgroups of } \mathrm{Aut}_F(K)\} \longrightarrow \{ \text{ subfields of K containing } F\}.$$

If $H_1 \subset H_2$, then every $x \in K$ that's fixed by H_2 is also fixed by H_1, so $L_{H_2} \subseteq L_{H_1}$. The above map is also inclusion-reversing.

Of course the natural question is whether these maps are inverses to each other. This is not always the case.

Example 8.1. If $F = \mathbb{Q}$, and $K = \mathbb{Q}(\sqrt[3]{2})$, then $\mathrm{Aut}_F(K)$ is trivial. Indeed, any map $\sigma : K \to K$ has to map $\sqrt[3]{2}$ to a root of $x^3 - 2$ in K. But $\sqrt[3]{2}$ is the only such root, the other two being complex. Therefore $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ necessarily. Since $\sigma|\mathbb{Q} = \mathrm{id}$, and K is generated by $\sqrt[3]{2}$ over $\mathbb{Q}$, $\sigma = \mathrm{id}$. This shows the map from subfields to subgroups can fail to be injective.

Example 8.2. Let p be an odd prime, $F = \mathbb{F}_p$, and $K = \mathbb{F}_{p^2}(\alpha)$, where $\alpha = t^{1/p}$. In other words K is $\mathbb{F}_{p^2}$ adjoined with a root of $f(x) = x^p - t$. Let $\sigma \in \mathrm{Aut}_F(K)$. Since K is generated by α over $\mathbb{F}_{p^2}$, σ is determined by $\sigma(\alpha)$, and the restriction $\sigma|_{\mathbb{F}_{p^2}}$ of σ to $\mathbb{F}_{p^2}$. Now $\mathbb{F}_{p^2}$ is the splitting field of

$$x^{p^2} - x = x(x^{p^2-1} - 1) = x(x^{\frac{p^2-1}{2}} - 1)(x^{\frac{p^2-1}{2}} + 1)$$

But we have seen that over K, $f(x) = (x - \alpha)^p$. Let $\sigma \in \mathrm{Aut}_F(K)$. which is just $\mathrm{Aut}(K)$ since F is the prime field. Then σ is determined by its restriction to $\mathbb{F}_{p^n}$, and $\sigma(\alpha)$. The restriction

Proposition 8.3. *Let $\sigma : F \to F'$ be a field isomorphism, K/F the splitting field of some $f(x) \in F[x]$, and K'/F' the splitting field of $g(x)$, the polynomial obtained by applying σ to $f(x)$. Then the number of extensions of σ to an isomorphism $K \to K'$ is at most $[K : F]$. If $f(x)$ is separable, it is exactly $[K : F]$.*

Proof. The proof is by induction on $n = [K : F]$. If $n = 1$, then $K = F$, $K' = F'$, and the unique extension of σ to $K \to K'$ is just σ.

Now assume the proposition holds for all fields extensions K/F of degree smaller than n. Let $f_0(x)$ be an irreducible factor of $f(x)$ over F, and $\alpha \in K$ a root of $f_0(x)$. Then $F(\alpha)$ is a subextension of K/F. If $\widetilde{\sigma} : K \to K'$ extends $\sigma : F \to F'$, then it maps α to a root β of some irreducible factor $g_0(x)$ of $g(x)$, and induces $\sigma_0 : F(\alpha) \to F(\beta)$. We know that $[F(\alpha) : F]$ is equal to the degree of $g(x)$. On the other hand, there are as many maps $F(\alpha) \to K$ as there are distinct roots of $g(x)$. Therefore there are at most $[F(\alpha) : F] = \deg(g)$ choices for $\sigma_0(\alpha)$, with equality if and only if $f_0(x)$ is separable. By induction, each such σ_0 has at most $[K : F(\alpha)]$ extensions to $\widetilde{\sigma} : K \to K'$. Since K is also the splitting field of $f(x)$ over $F(\alpha)$, there are exactly $[K : F(\alpha)]$ extensions if $f(x)$ is separable. Then altogether there are at most $[K : F(\alpha)][F(\alpha) : F] = [K : F]$ extensions for $\widetilde{\sigma}$, and exactly that many if $f(x)$ is separable. □

Corollary 8.4. *Let K/F be the splitting field of some $f[x] \in F[x]$. Then $|\mathrm{Aut}_F(K)| \leq [K : F]$, with equality if $f(x)$ is separable.*

Proof. Follows from the proposition for $F' = F$, $K = K'$, and $\sigma = \mathrm{id}$. □

9. Galois extensions

Let K/F be an extension, and $G = \mathrm{Aut}(K/F)$. To any subgroup $H < G$ we associated a field

$$K^H = \{a \in K : \sigma(a) = a \text{ for all } \sigma \in H\}.$$

Then $F \subset K^H \subset K$.

And to every $L \subset K$ containing F we associated $\mathrm{Aut}(K/L) \subset G$. Let us denote this group by $H(L)$ for short, and write

$$\mathrm{SubF}(K/F) = \{\text{subfields } L \subseteq K \text{ containing } F\}.$$
$$\mathrm{Sub(G)} = \{ \text{ subgroups } H < G\}.$$

Then we have maps

$$\mathrm{SubF}(K) \to \mathrm{SubG}(G), \quad L \mapsto H(L) \ \ (= \mathrm{Aut}(K/L)),$$

$$\mathrm{Sub}(G) \to \mathrm{SubF}(K), \quad H \mapsto K^H.$$

Definition 9.1. A finite extension K/F is called *Galois* if $\mathrm{Aut}(K/F) = [K : F]$. In that case $\mathrm{Aut}(K/F)$ is written $\mathrm{Gal}(K/F)$ and called the *Galois group* of the extension. If $f(x) \in F[x]$ is separable, the *Galois group* of $f(x)$ is $\mathrm{Gal}(K/F)$ for a splitting field K of $f(x)$.

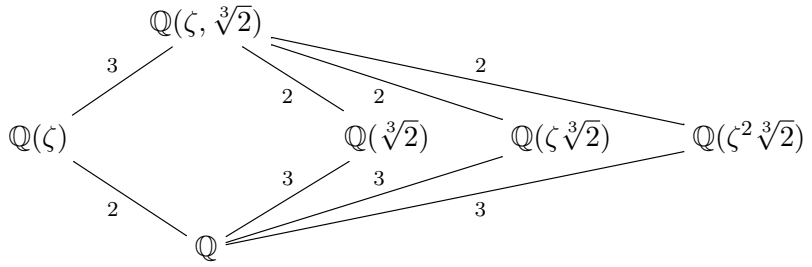
Example 9.2. Any quadratic extension $K = F(\sqrt{a})$ over a field F, $\mathrm{char}(F) \neq 2$, is Galois. That's because there is a non-trivial automorphism

$$\sigma : K \to K, \quad \sigma(x + \sqrt{a}y) = x - \sqrt{a}y.$$

Since $\mathrm{char}(F) \neq 2$, $-\sqrt{a} \neq \sqrt{a}$, so $\sigma \neq \mathrm{id}$. Then $|\mathrm{Aut}(K/F)| \geq 2 = [K : F]$ so $|\mathrm{Aut}(K/F)| = [K : F]$ by the corollary of the proposition we proved last time.

Example 9.3. Consider the extension $L = \mathbb{Q}(\zeta, \sqrt[3]{2})$ of $\mathbb{Q}$, where $\zeta = \zeta_3 = e^{2\pi i/3}$. Since it is the splitting field of $x^2 - 3$, it is Galois. Let $G = \mathrm{Aut}(L/\mathbb{Q})$ be the Galois group.

The diagram of subfields of L are



Any element $\sigma \in \mathrm{Aut}(L/\mathbb{Q})$ is determined by its value on ζ and on $\sqrt[3]{2}$. The possibilities for $\sigma(\sqrt[3]{2})$ are $\sqrt[3]{2}$, $\zeta\sqrt[3]{2}$ and $\zeta^2\sqrt[3]{2}$. For $\sigma(\zeta)$ the possibilities are ζ and ζ^2.

K is Galois over $\mathbb{Q}(\zeta)$, since it's the splitting field of $x^3 - 2$. Then $\mathrm{Aut}(K/\mathbb{Q}(\zeta))$, which is a subgroup of G must have order 3. Since an element of $\mathrm{Aut}(K/\mathbb{Q}(\zeta))$ is determined by its value on $\sqrt[3]{2}$, and the possibilities are $\sqrt[3]{2}$, $\zeta\sqrt[3]{2}$, and $\zeta^2\sqrt[3]{2}$, all three choices must actually give rise to elements of $\mathrm{Gal}(K/\mathbb{Q}(\zeta)$. Choose $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ to be the unique element for which

$$\sigma(\sqrt[3]{2}) = \zeta\sqrt[3]{2}, \quad \sigma(\zeta) = \zeta.$$

Then $\mathrm{Aut}(K/\mathbb{Q}(\zeta)) = \langle\sigma\rangle$.

Similarly, $\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2})$ is Galois, the Galois group has order two, and is generated by the unique automorphism τ such that

$$\tau(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \tau(\zeta) = \zeta^2.$$

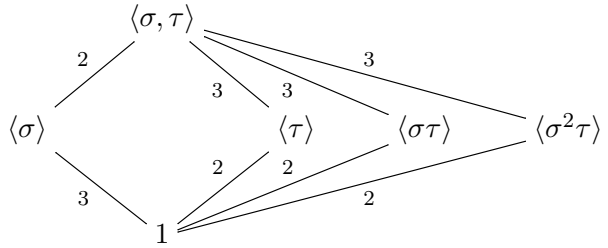
Since $\mathrm{Gal}(K/\mathbb{Q})$ has order six, it must be generated by σ and τ. Note that

$$\sigma\tau(\sqrt[3]{2}) = \sigma(\sqrt[3]{2}) = \zeta\sqrt[3]{2}, \quad \sigma\tau(\zeta) = \sigma(\zeta^2) = \zeta^2$$

and

$$\tau\sigma(\sqrt[3]{2}) = \tau(\zeta\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}, \quad \tau\sigma(\zeta) = \zeta^2.$$

Since $\sigma\tau \neq \tau\sigma$, $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to S_3. Then there are two other elements of order two in the group. From $\sigma\tau\sigma = \tau$ we see that they are $\tau\sigma$ and $\tau\sigma^2 = \sigma\tau$.



.

Here like in the subfield diagram the arrows indicate the index of a subgroup. Notice the similarity with the subgroup diagram. As the labels indicate, the orientation is upside down, so that the trivial group 1 corresponds to the entire extension K/F, and full automorphism group $\mathrm{Gal}(K/F)$ corresponds to $\mathbb{Q}/\mathbb{Q}$.

We want to prove a similar relationship exists between the field diagram of any Galois extension and the subgroup diagram of its Galois group.

Notice from the example diagrams that the size of a subgroup of $\mathrm{Gal}(K/F)$ coincides with the degree of K over the fixed field. For instance the fixed field of $\langle\sigma\rangle$ is $\mathbb{Q}(\zeta)$, and $[\mathbb{Q}(\zeta, \sqrt[3]{2}) : \mathbb{Q}] = 3 = |\langle\sigma\rangle|$.

To prove this fact, we need to establish a fundamental result about groups in general.

Definition 9.4. A *character* of a group G, with values in a field K, is a group homomorphism $\chi : G \to K^\times$.

The set of characters $\mathrm{Hom}(G, L^\times)$ of a group G is a subset of

$$\{f : G \to L \mid \text{set-theoretic function}\}$$

which is a vector space over L.

Lemma 9.5. *Let V be a vector space over a field K, and $S = \{v_1, \cdots, v_n\}$, a minimal set of non-zero linearly dependent vectors. In other words, any proper subset of S is linearly independent. Let $U \subset K^n$ consist of tuples $(a_1, \cdots, a_n)$ such that*

$$a_1 v_1 + \cdots + a_n v_n = 0.$$

Then $\dim_K U = 1$.

Proof. Since S is linearly dependent, there exists $(a_1, \cdots, a_n) \in U$ with some $a_i \neq 0$. Let $\phi : U \to K$ be the projection map $\phi(a_1, \cdots, a_n) = a_i$. Then ϕ is K-linear and non-zero, hence onto. Suppose $(b_1, \cdots, b_n) \in \ker(\phi)$, so that $b_i = 0$. Then

$$b_1 v_1 + \cdots + b_{i-1} v_{i-1} + b_{i+1} v_{i+1} + \cdots + b_n v_n = 0.$$

But since S is a minimal linearly dependent set, $\{v_1, \cdots, v_{i-1}, v_{i+1}, \cdots, v_n\}$ is linearly independent, hence $b_1 = b_2 = \cdots = b_n = 0$. Therefore $\ker(\phi) = 0$, ϕ is an isomorphism, and $\dim_K U = 1$. □

Theorem 9.6. *Distinct characters $\chi_1, \cdots, \chi_n$ of a group G are linearly independent, (as functions $G \to L$.)*

Proof. Assume on the contrary that χ_i are linearly dependent. Without loss of generality we may also assume they are a minimal such set of characters.

Let $U \subset K^n$ be the set of all $(a_1, \cdots, a_n)$ such that

$$a_1 \chi_1 + \cdots + a_n \chi_n = 0$$

as functions on G.

Let $(a_1, \cdots, a_n) \in U$ be a non-zero vector, so that $a_i \neq 0$ for some i. Let $h \in G$. For any $g \in G$, if we evaluate the relation above on hg, and use the fact that χ_i are characters, we obtain

$$a_1 \chi_1(h)\chi_1(g) + \cdots + a_n \chi_n(h)\chi_n(g) = 0.$$

Since this is true for all h, we get

$$(\chi_1(h)a_1, \cdots, \chi_n(h)a_n) \in U \Longrightarrow (\frac{\chi_1(h)}{\chi_i(h)}a_1, \frac{\chi_2(h)}{\chi_i(h)}a_2, \cdots, a_i, \cdots, \frac{\chi_n(h)}{\chi_i(h)}a_n) \in U.$$

By the lemma, U is one-dimensional. Then comparing the above with $(a_1, \cdots, a_n) \in U$ and using $a_i \neq 0$ we get for all $j = 1, \cdots, n$,

$$\forall h \in H, \quad \frac{\chi_j(h)}{\chi_i(h)} a_j = a_j.$$

Since $\chi_1, \cdots, \chi_n$ are all distinct, this can only be true if $a_j = 0$, for $j \neq i$. Then $a_i \chi_i = 0 \Longrightarrow \chi_i = 0$, which is absurd because χ_i takes values in $K^\times$. □

The relevance of this theorem to us is as follows. If $\sigma : K \to L$ is a field embedding, it may be considered as character of the group $K^\times$ with values in $L^\times$. Note $\sigma|_{K^\times}$ determines σ, since $\sigma(0) = 0$.

Corollary 9.7. *Distinct embeddings $\sigma_1, \cdots, \sigma_n$ of a field K into another field L are linearly independent over L.*

Proposition 9.8. *Let H be a finite subgroup of $\mathrm{Aut}(K)$, and $F = K^H$. Then $|H| \leq [K : F]$.*

Proof. Let $n = |H|$, and $m = [K : F]$, and assume $n > m$.

Let $\alpha_1, \cdots, \alpha_m$ be an F-basis for K. Define an $m \times n$ matrix $A = (a_{ij})$ by setting $a_{ij} = \sigma_j(\alpha_i)$, so

$$A = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \cdots & \cdots & \sigma_n(\alpha_2) \\ \vdots & & & \vdots \\ \sigma_1(\alpha_m) & \cdots & \cdots & \sigma_n(\alpha_m) \end{pmatrix}$$

For $(d_1, \cdots, d_m) \in F^m$, let D be the $1 \times m$ matrix $(d_1, \cdots, d_m)$. Then DA is a $1 \times n$ matrix with jth entry

$$\sum_{i=1}^{m} d_i \sigma_j(\alpha_i) = \sum_{i=1}^{m} \sigma_j(d_i \alpha_i) = \sigma_j(\sum_{i=1}^{m} d_i \alpha_i).$$

If $n > m$ the matrix A is singular, so there is a non-zero column vector $\underline{c} = (c_1, \cdots, c_n)$ such that

$$A\underline{c} = 0.$$

That implies $DA\underline{c} = 0$, which is to say

$$c_1\sigma_1(a) + c_2\sigma_2(a) + \cdots + c_m\sigma_m(a) = 0, \quad a = \sum_{i=1}^{m} d_i\alpha_i.$$

But since α_i form a basis of K over F, *any* $a \in K$ has the form $\sum_{i=1}^{m} d_i\alpha_i$ for some d_i. Then the above equation says

$$c_1\sigma_1 + \cdots + c_m\sigma_m = 0$$

which contradicts the fact that $\sigma_1, \cdots, \sigma_m$ are linearly independent. □

In fact we will also show the reverse inequality $|H| \geq [K : F]$.

Same proof:

Let $\alpha = (\alpha_1, \cdots, \alpha_m) \in K^m$, and write $\sigma\alpha$ for $(\sigma\alpha_1, \cdots, \sigma\alpha_m)$. Then $\sigma_1\alpha, \cdots, \sigma_n\alpha$ are n vector in K^m. If $n > m$, there exist $c_i \in K$ such that $\sum_{i=1}^{n} c_i\sigma_i\alpha = 0$. Writing this out, this means

$$\sigma(\alpha_1) = \sigma(\alpha_2) = \cdots = \sigma(\alpha_m) = 0,$$

where $\sigma = \sum_{i=1}^{n} c_i\sigma_i$ is an F-linear function $K \to K$. If $\alpha_1, \cdots, \alpha_m$ are an F-basis for K, $\sigma(\alpha_i) = 0$ implies $\sigma = 0$. But $\sum_{i=1}^{n} c_i\sigma_i = 0$ for c_i not all zero contradicts the independence of characters.

10. Galois Extensions II

We now want to prove the reverse inequality of the proposition from last time.

Proposition 10.1. *Let H be a finite subgroup of $\mathrm{Aut}(K)$, and $F = K^H$. Then $|H| \geq [K : f]$.*

Proof. Let $n = |H|$, $m = [K : F]$ and assume that $n < m$.

Let $\alpha = (a_1, \cdots, a_m) \in K^m$ be linearly independent, and suppose $H = \{\sigma_1, \cdots, \sigma_n\}$. Write $\alpha_i = (\sigma_1 a_i, \sigma_2 a_i, \cdots, \sigma_n a_i) \in K^n$, for $i = 1, \cdots, m$. Since $m > n$, the α_i must be linearly dependent. Pick a minimal linearly dependent subset of α_i, and by relabeling if necessary assume they are $\alpha_1, \cdots, \alpha_r$. Now let $V \subset K^r$ be the subspace consisting of all $(c_1, \cdots, c_r)$, such that $\sum_i c_i\alpha_i = 0$.

Now observe that if $(c_1, \ldots, c_r) \in V$, for $\sigma \in H$, $(\sigma c_1, \cdots, \sigma c_r)$ is also in V. Indeed if $(c_1, \cdots, c_r) \in V$, then

$$\sum_{i=1}^{r} c_i\alpha_i = (\sum_{i=1}^{r} c_i\sigma_1(a_i), \cdots, \sum_{i=1}^{r} c_i\sigma_n(a_i)) = 0.$$

For $\sigma \in H$, and each $j = 1, \cdots, n$, we have

$$\sum_{i=1}^{r} c_i\sigma_j(a_i) = 0 \iff \sigma(\sum_{i=1}^{r} c_i\sigma_j(a_i)) = 0 \iff \sum_{i=1}^{r} \sigma(c_i)(\sigma\sigma_j)(a_i) = 0.$$

Now $\{\sigma\sigma_1, \cdots, \sigma\sigma_n\} = \{\sigma_1, \cdots, \sigma_n\} = H$. Therefore

$$\sum_{i=1}^{r} \sigma(c_i)\sigma\sigma_j(a_i)) = 0,\ j = 1, \cdots, n \iff \sum_{i=1}^{r} \sigma(c_i)\sigma_j(a_i) = 0,\ j = 1, \cdots, n.$$

In other words,

$$(c_1, \cdots, c_r) \in V \iff (\sigma(c_1), \cdots, \sigma(c_r)) \in V.$$

Now by Lemma 9.5, $\dim_K V = 1$. Let $(c_1, \cdots, c_r) \in V$ be non-zero, and wolog assume $c_1 = 1$. Now for each $\sigma \in H$, we have

$$(\sigma 1, \sigma c_2, \cdots, \sigma c_r) = (1, \sigma c_2, \cdots, \sigma c_r).$$

Since $\dim_K V = 1$, $(1, \sigma c_2, \cdots, \sigma c_r)$ must be proportional to $(1, c_2, \cdots, c_r)$. But that implies $\sigma c_i = c_i$ for all i, and all $\sigma \in H$. Then $c_i \in F$ by definition of F. Then we have

$$\sum_{i=1}^{r} c_i\sigma_j(a_i) = 0 \Longrightarrow \sigma\left(\sum_{i=1}^{r} c_i a_i\right) = 0 \Longrightarrow \sum_{i=1}^{r} c_i a_i = 0.$$

which contradicts the linear independence of a_i. □

Now putting Propositions 9.8 and 10.1 together, we have proven the following theorem.

Theorem 10.2. *Let K be a field, H be a finite subgroup of $\mathrm{Aut}(K)$, and $F = K^H$. Then*

$$|H| = [K : F].$$

The first application is to generalize Corollary 8.4.

Corollary 10.3. *For any finite extension K/F, $|\mathrm{Aut}(K/F)| \leq [K : F]$. Equality holds, i.e. K/F is Galois, if and only if $F = K^{\mathrm{Aut}(K/F)}$.*

Proof. For $H = \mathrm{Aut}(K/F)$, we have $F \subseteq K^H$. By the theorem,

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

with equality holding if and only if $[K^H : F] = 1$. □

Corollary 10.4. *Let K be a field, H a finite subgroup of $\mathrm{Aut}(K)$. Then $\mathrm{Aut}(K/K^H) = H$. In particular, K/K^H is Galois.*

Proof. Let $F = K^H$. By definition, $H < \mathrm{Aut}(K/F)$, so $|H| \leq |\mathrm{Aut}(K/F)|$. By the previous corollary, $|\mathrm{Aut}(K/F)| \leq [K : F]$, and by the theorem $[K : F] = |H|$. Altogether this shows $|\mathrm{Aut}(K/F)| = |H|$, therefore $\mathrm{Aut}(K/F) = H$. From $|\mathrm{Aut}(K/F)| = |H| = |[K : F]|$ we deduce K/F is Galois. □

Let K be a field. The previous corollary says the composition

$$\{\text{finite subgroups of } \mathrm{Aut}(K)\} \longrightarrow \{\text{subfields of } K\} \longrightarrow \{\text{finite subgroups of } \mathrm{Aut}(K)\}.$$

$$H \longmapsto K^H \longmapsto \mathrm{Aut}(K/K^H)$$

is the identity. In particular the first map is injective. In other words,

Corollary 10.5. *For distinct finite subgroups H_1, H_2 of $\mathrm{Aut}(K)$, K^{H_1} and K^{H_2} are distinct.*

If K/F is Galois, and $\alpha \in K$, elements of the form $\sigma\alpha$ for $\sigma \in \mathrm{Gal}(K/F)$ are called the *Galois conjugates* of α. They are the orbit of α under the action of $\mathrm{Gal}(K/F)$ on K.

Theorem 10.6. *Let K/F be Galois, $G = \mathrm{Gal}(K/F)$, and $f(x) \in F[x]$ an irreducible polynomial. If $f(\alpha) = 0$ for some $\alpha \in K$, then*

$$f(x) = \prod_{\beta \in G\alpha} (x - \beta),$$

where $G\alpha$ is the set of conjugates of α. In particular, $f(x)$ is separable and splits over K.

Proof. Let

$$g(x) = \prod_{\beta \in G\alpha} (x - \beta).$$

The action of G permutes the elements of $G\alpha$, so for $\sigma \in \mathrm{Gal}(K/F)$ we have

$$\sigma(g(x)) = \prod_{\beta \in G\alpha} (x - \sigma(\beta)) = g(x).$$

Then the coefficients of $g(x)$ are invariant under each $\sigma \in \mathrm{Gal}(K/F)$, hence lie in the fixed field $K^{\mathrm{Gal}(K/F)}$, which is F by Corollary 10.3. Therefore $g(x) \in F[x]$.

Since $f(x)$ is the minimal polynomial of α over F, and $g(\alpha) = 0$, we have $f(x)|g(x)$. On the other hand, every root of $g(x)$ is also a root of $f(x)$ and the roots of $g(x)$ are distinct, hence $g(x)|f(x)$. Therefore $f(x) = g(x)$, and all the roots of $f(x)$ are in K. Since $g(x)$ is separable, so is $f(x)$. □

As an application, we obtain another characterization of Galois extensions.

Corollary 10.7. *A finite extension K/F is Galois if and only if K is the splitting field of a separable $f(x) \in F[x]$.*

Proof. Let $\alpha_1, \cdots, \alpha_n$ be an F-basis for K and $G = \mathrm{Gal}(K/F)$. Each α_i has a Galois orbit $G\alpha_i \subset K$. Wolog let $G\alpha_1, \cdots, G\alpha_r$, for $r \leq n$, be the distinct Galois orbits, and put

$$f_i(x) = \prod_{\beta \in G\alpha_i} (x - \beta), \quad f = \prod_{i=1}^{r} f_i(x).$$

By the theorem, each $f_i(x)$ is in $f(x)$, separable, and splits over K. Since $G\alpha_i$, $i = 1, \cdots, r$ are distinct orbits, they are also disjoint, therefore $f(x)$ is also separable. Now $\alpha_1, \cdots, \alpha_n \in \cup_{i=1}^{r} G\alpha_i$, so $f(\alpha_i) = 0$ for all i. This shows K is the splitting field of $f(x)$. □

Let us summarize our characterizations of Galois groups so far.

Definition 10.8. A field extension K/F is called *normal* if K is the splitting field of a collection of polynomials $f_i(x) \in F[x]$.

Proposition 10.9. *Let K/F be a finite extension. The following are equivalent:*

(i) *K/F is Galois.*
(ii) $[K : F] = |\mathrm{Aut}(K/F)|$
(iii) *F is the fixed field of $\mathrm{Aut}(K/F)$ in K.*
(iv) *K is the splitting field of a separable polynomial $f(x) \in F[x]$.*
(v) *K is a normal, separable extension.*

Proof. *(i)* $\iff$ *(ii)* is by definition. Corollary 10.3 provides the equivalence of *(i)* with *(iii)* and *(iv)*. It's clear that *(iv)* implies *(v)*. If K is normal, it is the splitting field of some $f_i(x)$, which can be taken to be irreducible and distinct. If K is also separable, each $f_i(x)$ is separable, hence *(v)* is the splitting field of $f(x) = \prod_i f_i(x)$, which is separable as $f_i(x)$ are distinct, irreducible, and separable. This shows *(v)* $\implies$ *(iv)*. □

11. Fundamental theorem of Galois theory

Let K/F be a finite extension. Recall the *Galois correspondence*

$$\{\text{subgroups of } \mathrm{Aut}(K/F)\} \longrightarrow \{\text{subfields } L \subset K \text{ containing F }\}$$
$$H \longmapsto K^H$$

and

$$\{\text{subfields } L \subset K \text{ containing F }\} \longrightarrow \{\text{subgroups of } \mathrm{Aut}(K/F)\}$$
$$L \longmapsto \mathrm{Aut}(K/L).$$

In Corollary 10.4, we showed that the composition $H \mapsto K^H \mapsto \mathrm{Aut}(K/K^H)$ is the identity. As we have seen in examples, the reverse composition $L \mapsto \mathrm{Aut}(K/L) \mapsto K^{\mathrm{Aut}(K/L)}$ may be not be identity, as $K^{\mathrm{Aut}(K/L)}$ may be strictly larger than L. For instance for $K = \mathbb{Q}(\sqrt[3]{2})$ over $F = \mathbb{Q}$, we saw that $\mathrm{Aut}(K/F) = 1$, so that $K^{\mathrm{Aut}(K/F)} = K \supsetneq F$.

Proposition 11.1. *The Galois correspondence is a bijection if and only if K/F is Galois. In particular if K/F is Galois, so is K/L for all $L \subset K$ containing F*

Proof. Let $L/F \subset K/F$. By Proposition 10.9, $K^{\mathrm{Aut}(K/L)} = L$ if and only if K/L is Galois. Thus the Galois correspondence is a bijection if and only if K/L for every $L \subset K$ containing F. In particular, it's necessary that K/F be Galois.

Conversely, suppose K/F is Galois. By Proposition 10.9, K is the splitting field of a separable $f(x) \in F[x]$. Then K is again the splitting field of $f(x) \in L[x]$, so K/L is Galois. Therefore every K/L is Galois. □

Thus K/F is Galois exactly when the lattice diagram of subextensions $L/F \subset K/F$ coincides with the lattice diagram of subgroups of $\mathrm{Gal}(K/F)$. More precisely:

Proposition 11.2. *Let K/F be Galois, and $G = \mathrm{Gal}(K/F)$. Let H_1, H_2 be subgroups corresponding to subfields L_1, L_2. Then*

(i) *$H_1 \subseteq H_2$ if and only if $L_2 \subseteq L_1$, and in that case $[L_1 : L_2] = [H_2 : H_1]$. In particular,*
(ii) *$[K : K^H] = |H|$ and $[K^H : F] = [G : H]$ for every subgroup $H \subset G$.*
(iii) *Let $\langle H_1, H_2\rangle$ denote the subgroup of G generated by H_1 and H_2, and let L_1L_2 be the composite of L_1 and L_2 in K. Then*

$$K^{\langle H_1,H_2\rangle} = L_1 \cap L_2, \quad H_1 \cap H_2 = \mathrm{Aut}(K/L_1L_2).$$

Proof. First we prove (ii). Let $H < G$. By Proposition 11.1, K/K^H is Galois, therefore by Proposition 10.9, $|H| = |\mathrm{Aut}(K/K^H)| = [K : K^H]$. Since K/F is Galois, we also have $|G| = [K : F]$. Then $[K^H : F] = [K : F]/[K : K^H] = |G|/|H| = [G : H]$.

The first part of (i) we have already seen, that the Galois correspondence is order-reversing. For the second part, suppose $H_1 \subseteq H_2$, so that $K^{H_2} \subseteq K^{H_1}$. We have

$$[K^{H_1} : K^{H_2}] = [K^{H_1} : F]/[K^{H_2} : F] = [G : H_1]/[G : H_2] = [H_2 : H_1].$$

For (iii), since L_1, $L_2 \subseteq L_1L_2$, we have $\mathrm{Aut}_F(K/L_1L_2) \subset H_1 \cap H_2$. Conversely, if $\sigma \in H_1 \cap H_2$, it fixes L_1 and L_2. Since L_1L_2 is generated by L_1 and L_2 over F, σ also fixes L_1L_2. Therefore $\mathrm{Gal}(K/L_1L_2) = H_1 \cap H_2$.

The groups H_1 and H_2 both fix $L_1 \cap L_2$, so $\langle H_1, H_2\rangle \subset \mathrm{Gal}(K/L_1 \cap L_2)$, hence $L_1 \cap L_2 \subset K^{\langle H_1,H_2\rangle}$. On the other hand $K^{\langle H_1,H_2\rangle} \subset K^{H_i} = L_i$, for $i = 1, 2$, so $K^{\langle H_1,H_2\rangle} = L_1 \cap L_2$. □

For a finite extension L/F, we have seen that in general $|\mathrm{Aut}_F(L)| \leq [L : F]$, with equality if and only if L/F is Galois. Next we want to clarify where the "missing automorphisms" go when L/F is not Galois.

Recall that for field extensions L_1/F and L_2/F, we write $\mathrm{Hom}_F(L_1, L_2)$ for the set of field embeddings $\sigma : L_1 \hookrightarrow L_2$ such that $\sigma|_F = \mathrm{id}$.

Let K/F be a Galois field extension, and $F \subseteq L \subseteq K$. Let $\overline{K}$ denote a fixed algebraic closure of K, which we previously proved always exists.

Lemma 11.3. $\mathrm{Hom}_F(L, \overline{K}) = \mathrm{Hom}_F(L, K)$. *In other words, every F-linear field embedding $\sigma : L \hookrightarrow \overline{K}$ has image contained in K.*

Proof. Let $\sigma \in \mathrm{Hom}_F(L, \overline{K})$. For each $\alpha \in L$, the minimal polynomial $m_\alpha(x)$ of α over F splits completely over K, since K/F is Galois. Then $m_\alpha(\sigma\alpha) = 0$, therefore $\sigma\alpha \in K$. □

For each $\sigma \in \mathrm{Hom}_F(L, \overline{K})$, we denote $\sigma(L)$ by L^σ. By the Lemma, $F \subset L^\sigma \subset K$.

Proposition 11.4. *Let K/F be Galois, $G = \mathrm{Gal}(K/F)$, and $L = K^H$, for $H \subset G$. The map*

$$\mathrm{Gal}(K/F) \to \mathrm{Hom}_F(L, K), \quad \sigma \mapsto \sigma|_L$$

is surjective, and induces a bijection

$$G/H \longleftrightarrow \mathrm{Hom}_F(L, K).$$

Then L/F is Galois if and only if H is normal, if and only if $\mathrm{Hom}_F(L, K) = \mathrm{Aut}_F(L)$. In that case the above bijection is a group isomorphism $G/H \simeq \mathrm{Gal}(L/F)$

Proof. Let $\sigma :\in \mathrm{Hom}_F(L, K)$. Then σ is an isomorphism $L \to L^\sigma \subset K$ of extensions of F. Since K/F is Galois, it's the splitting field of some $f(x) \in F[x]$. Then K/L is the splitting field of $f(x) \in L[x]$, as well as the splitting field of $f^\sigma(x) \in L^\sigma[x]$ over L^σ, since $f(x) = f^\sigma(x)$. By the theorem on extension of isomorphisms, $\sigma : L \xrightarrow{\sim} L^\sigma$ may be extended to an isomorphism $\tau : K \to K$. This shows the map

$$\mathrm{Gal}(K/F) \to \mathrm{Hom}_F(L, K), \quad \tau \mapsto \tau|_L,$$

is *surjective*. Now suppose τ_1, τ_2 are in $\mathrm{Gal}(K/F)$, and $\tau_1|_L = \tau_2|_L$. In particular, $L^{\tau_1} = L^{\tau_2}$, and $(\tau_2|_L)^{-1}(\tau_1|_L) = (\tau_2^{-1}\tau_1)|_L = \mathrm{id}_L$, so $\tau_2^{-1}\tau_1 \in \mathrm{Gal}(K/L)$. Conversely if $\tau_2^{-1}\tau_1 \in \mathrm{Aut}_F(K)$ fixes L, then $\tau_2^{-1}|_{L^{\tau_1}} : L^{\tau_1} \xrightarrow{\sim} L$, which implies $L^{\tau_2} = L^{\tau_1}$ and $\tau_1|_L = \tau_2|_L$. This shows for $\tau_1, \tau_2 \in \mathrm{Gal}(K/F)$, $\tau_1|_L = \tau_2|_L$ if and only if $\tau_1\mathrm{Gal}(K/L) = \tau_2\mathrm{Gal}(K/L)$ as cosets. Thus the restriction map $\tau \mapsto \tau|_L$ induces a bijection

$$\mathrm{Gal}(K/F)/\mathrm{Gal}(K/L) \to \mathrm{Hom}_F(L, K).$$

In particular, if $H = \mathrm{Gal}(K/L)$ so that $L = K^H$, we get $[L : F] = [G : H] = |\mathrm{Hom}_F(L, K)|$. Since $\mathrm{Aut}_F(L) \subseteq \mathrm{Hom}_F(L, K)$, it follows that L/F is Galois if and only if $\mathrm{Aut}_F(L) = \mathrm{Hom}_F(L, K)$.

Suppose L/F is Galois, so that $\mathrm{Hom}_F(L, K) = \mathrm{Gal}(L/F)$. Then the restriction $\tau \mapsto \tau|_L$ is a surjective group homomorphism $G \to \mathrm{Gal}(L/F)$ with kernel H, so H is normal, inducing $G/H \xrightarrow{\sim} \mathrm{Gal}(L/F)$. Conversely, suppose $H = \mathrm{Gal}(K/L)$ is normal in $\mathrm{Gal}(K/F)$. For $\sigma \in \mathrm{Gal}(K/F)$, we have $\mathrm{Gal}(K/L^\sigma) = \sigma\mathrm{Gal}(K/L)\sigma^{-1} = \mathrm{Gal}(K/L)$. Thus L and L^σ coincide, both being fixed fields of $\mathrm{Gal}(K/L)$. In particular, $\sigma|_L(L) = L$, so that $\mathrm{Hom}_F(K, L) = \mathrm{Aut}_F(L)$. Therefore $[L : F] = |\mathrm{Aut}_F(L)|$, and L/F is Galois. □

The proposition shows that $|\mathrm{Hom}_F(L, K)| = [L : F]$ for all subfields L of K containing F. Then L/F is Galois if and only if every F-linear embedding $L \hookrightarrow K$ has image L.

We now summarize what we have proved.

Theorem 11.5 (Fundamental Theorem of Galois Theory)**.** *Let K/F be a finite Galois extension. The correspondence*

$$\{\textit{subgroups of } \mathrm{Gal}(K/F)\} \longrightarrow \{\textit{subfields } L \subset K \textit{ containing } F\}$$

$$H \longmapsto K^H$$

and

$$\{\textit{subfields } L \subset K \textit{ containing } F\} \longrightarrow \{\textit{subgroups of } \mathrm{Gal}(K/F)\}$$

$$L \longmapsto \mathrm{Aut}(K/L) \subset \mathrm{Gal}(K/F)$$

is a bijection satisfying the following properties.

(i) *$F \subset L_1 \subseteq L_2 \subseteq K$ if and only if $\mathrm{Aut}(K/L_2) \subseteq \mathrm{Aut}(K/L_1)$*

(ii) *If $H \mapsto K^H = L$ under the correspondence,*

(1) K/L is Galois and $\mathrm{Gal}(K/L) = H$.

(2) L/F is Galois if and only if H is normal, in which case $\mathrm{Gal}(L/F) \cong G/H$.

(ii) *The Galois correspondence*

$$\begin{array}{ccc} 1 & \cdots\cdots\cdots\cdots\cdots\cdots\succ & K \\ \Big| & & \Big| \\ |H| & & [K:K^H] \\ \Big| & & \Big| \\ H & \cdots\cdots\cdots\cdots\cdots\cdots\succ & K^H \\ \Big| & & \Big| \\ [G:H] & & [L:F] \\ \Big| & & \Big| \\ G & \cdots\cdots\cdots\cdots\cdots\cdots\succ & F \end{array}$$

preserves the index. In other words $[K : K^H] = |H|$, *and* $[G : H] = [K^H : F]$.

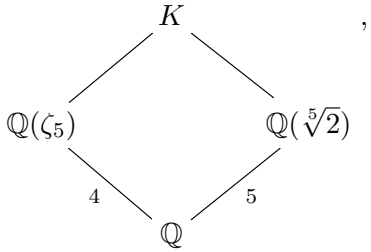
(ii) *Let* $L_1 = K^{H_1}$, $L_2 = K^{H_2}$, *then*

$$L_1 \cap L_2 = K^{\langle H_1, H_2\rangle}, \quad L_1 L_2 = K^{H_1 \cap H_2},$$

where $\langle H_1, H_2\rangle$ *is the subgroup of* G *generated by* H_1 *and* H_2, *and* L_1L_2 *is the composite of* L_1 *and* L_2.

12. Example of the Galois correspondence

Example 12.1. Let $K/\mathbb{Q}$ be the splitting field of $x^5 - 2$. The roots are $\zeta_5^a \sqrt[5]{2}$, $a = 1, \cdots, 5$. It follows that $K = \mathbb{Q}(\zeta_5, \sqrt[5]{2})$. From the diagram



,

we see that 4 and 5 must divide $[K : \mathbb{Q}]$, hence $[K : \mathbb{Q}] \geq 20$.

On the other hand, if $\sigma \in \mathrm{Aut}(K)$, then σ is determined by

$$\sigma(\zeta_5) \in \{\zeta_5, \cdots, \zeta_5^4\}, \quad \sigma(\sqrt[5]{2}) \in \{\sqrt[5]{2}, \zeta_5\sqrt[5]{2}, \cdots, \zeta_5^4\sqrt[5]{2}).$$

There are at most 20 choices for σ, so $\mathrm{Aut}(K) \leq 20$. Since K is Galois, we must have $[K : \mathbb{Q}] = \mathrm{Aut}(K) = 20$. In particular, each possibility for σ above does occur.

$G = \mathrm{Gal}(K/\mathbb{Q})$ is then generated by τ and σ where

$$\sigma(\zeta_5) = \zeta_5, \quad \sigma(\sqrt[5]{2}) = \zeta_5\sqrt[5]{2},$$
$$\tau(\zeta_5) = \zeta_5^2, \quad \tau(\sqrt[5]{2}) = \sqrt[5]{2}.$$

The subgroups $\langle\sigma\rangle$ and $\langle\tau\rangle$ have orders 5 and 4, respectively. Since $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ is Galois, $H = \mathrm{Gal}(K/\mathbb{Q}(\zeta_5))$ is normal in G. It has order 5, since $[K : \mathbb{Q}(\zeta_5)] = [K : \mathbb{Q}]/[\mathbb{Q}(\sqrt[5]{2})/\mathbb{Q}] = 20/4$. Then $H = \langle\sigma\rangle$, and $G = H \rtimes \langle\tau\rangle$. Thus to determine G it's enough to compute $\tau\sigma\tau^{-1}$.

$$\tau\sigma\tau^{-1}(\zeta_5) = \tau\sigma(\zeta_5^3) = \tau(\zeta_5^3) = \zeta_5, \quad \tau\sigma\tau^{-1}(\sqrt[5]{2}) = \tau\sigma(\sqrt[5]{2}) = \tau(\zeta_5\sqrt[5]{2}) = \zeta_5^2\sqrt[5]{2}.$$

It follows that $\tau\sigma\tau^{-1} = \sigma^2$. Then

$$G = \langle\sigma, \tau | \sigma^5 = \tau^4 = 1,\ \tau\sigma\tau^{-1} = \sigma^2\rangle.$$

This is called the general affine group of degree 1 over $\mathbb{F}_5$.

G has a subgroup of order 10, namely $I = \langle\sigma\rangle \rtimes \langle\tau^2\rangle$, which is isomorphic to D_5, the dihedral group with 10 elements, since $\tau^2\sigma\tau^{-2} = \sigma^4 = \sigma^{-1}$. This subgroup is unique, since any other subgroup of order 10 must contain the unique subgroup $\langle\sigma\rangle$ of order 5, so it must correspond to a

subgroup of order two in $G/\langle\sigma\rangle$. The latter is isomorphic to $\langle\tau\rangle$, so is cyclic of order 4, and has a unique subgroup of order 2.

Since $\langle\sigma\rangle \subset I$, $K^I \subset K^{\langle\sigma\rangle} = \mathbb{Q}(\zeta_5)$. Indeed K^I must be the unique quadratic subfield of $\mathbb{Q}(\zeta_5)$.

Claim: $K^I = \mathbb{Q}(\sqrt{5})$.

Let $x = a_0 + a_1\zeta_5 + a_2\zeta_5^2 + a_3\zeta_5^3 + a_4\zeta_5^4 \in \mathbb{Q}(\sqrt{5})$, with $a_i \in \mathbb{Q}$. Note K^I is the subfield of $\mathbb{Q}(\zeta_5)$ fixed by $\langle\tau^2\rangle$. We have

$$\tau^2(x) = a_0 + a_1\zeta_5^4 + a_2\zeta_5^3 + a_3\zeta_5^2 + a_4\zeta_5$$

so

$$\tau^2(x) = x \iff a_2 = a_3,\ a_1 = a_4.$$

Then $x = a_0 + a_1(\zeta_5 + \zeta_5^{-1}) + a_2(\zeta_5^2 + \zeta_5^{-2})$. In fact $(\zeta_5 + \zeta_5^{-1})^2 = \zeta_5^2 + \zeta_5^{-2} + 2$, so

$$K^I = \mathbb{Q}(\zeta_5 + \zeta_5^{-1}).$$

Exercise: Show $\mathbb{Q}(\zeta_5 + \zeta_5^{-1}) = \mathbb{Q}(\sqrt{5})$.

Any other subgroup of G must have order 4 or 2. If an element $\sigma^a\tau^b$ has order two, then

$$1 = \sigma^a\tau^b\sigma^a\tau^b.$$

Since $\tau\sigma\tau^{-1} = \sigma^2$, we have $\tau^b\sigma\tau^{-b} = \sigma^{2b}$, hence $\tau^b\sigma^a\tau^{-b} = \sigma^{2ab}$, $\tau^b\sigma^a = \sigma^{2ab}\tau^b$ and

$$1 = \sigma^a\tau^b\sigma^a\tau^b = \sigma^{2ab+a}\tau^{2b}.$$

Then $\tau^{2b} = 1 \Longrightarrow b = 2$ and $\sigma^{2ab+a} = \sigma^{5a} = 1$, which is true for any a. Then the subgroups of order two in G are

$$\langle\sigma^a\tau^2\rangle, \quad a = 0, 1, \cdots, 4.$$

We have

$$\sigma^a\tau^2(\sqrt[5]{2}) = \sigma^a(\sqrt[5]{2}) = \zeta_5^a\sqrt[5]{2}, \quad \sigma^a\tau^2(\zeta_5) = \sigma^a(\zeta_5^4) = \zeta_5^{-1}$$

It follows that $\sigma^a\tau^2$ fixes $\zeta_5 + \zeta_5^{-1}$, hence also $\sqrt{5}$, and that

$$\sigma^a\tau^2(\zeta_5^{3a}\sqrt[5]{2}) = \zeta_5^{3a}\sqrt[5]{2}, \quad \text{for } a = 1, \cdots, 5.$$

Then the fixed field of $\langle\sigma^a\tau^2\rangle$ contains $\mathbb{Q}(\sqrt{5}, \zeta_5^{3a}\sqrt[5]{2})$, over which $\mathbb{Q}(\zeta_5, \sqrt[5]{2})$ has degree 2. Then $\mathbb{Q}(\sqrt{5}, \zeta_5^{3a}\sqrt[5]{2})$ must be $K^{\langle\sigma^a\tau^2\rangle}$.

Now suppose $\sigma^a\tau^b$ has order 4. Then $(\sigma^a\tau^b)^2 = \sigma^{2a+b}\tau^{2b}$ must be one of the elements of order 2 from before. This is the case if and only if $2b \equiv 2 \pmod 4$ so $b = 1$ or $b = -1$. For $b = 1$, the elements of order 4 are

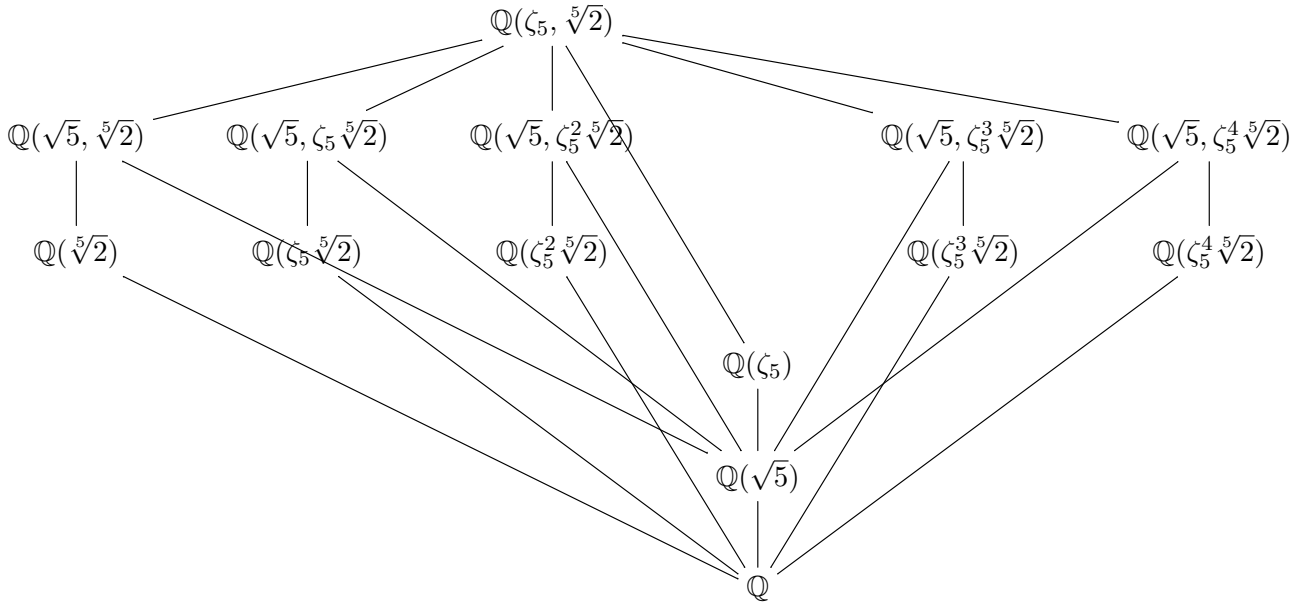
$$\sigma^a\tau, \quad a = 1, \cdots, 4$$

whose squares are $\sigma^{3a}\tau^2$. The elements of order 4 with $b = 3$ correspond to their inverses.

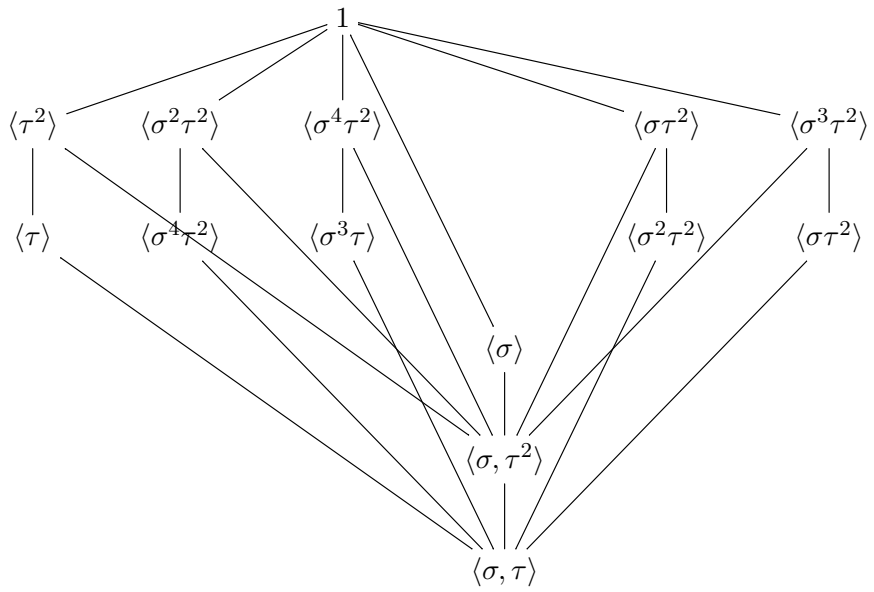
It follows that each element $\sigma^a\tau^2$ of order 2 is contained in a unique cyclic subgroup of order 4, generated by $\sigma^{2a}\tau$. Each such subgroup corresponds to the unique subfield of $\mathbb{Q}(\sqrt{5}, \zeta_5^{3a}\sqrt[5]{2})$ of index 2, namely $\mathbb{Q}(\zeta_5^{3a}\sqrt[5]{2})$. Indeed,

$$\sigma^{2a}\tau(\zeta_5^{3a}\sqrt[5]{2}) = \sigma^{2a}(\zeta_5^{6a}\sqrt[5]{2}) = \zeta_5^{8a}\sqrt[5]{2} = \zeta_5^{3a}\sqrt[5]{2}.$$

The subfields of K are therefore



corresponding to the lattice of subgroups



13. Galois theory of Finite Fields

Previously we showed that every finite field is isomorphic to some $\mathbb{F}_{p^n}$, and that subfields of $\mathbb{F}_{p^n}$ are $\mathbb{F}_{p^d}$ for $d|n$. Armed with Galois theory we can clarify this relationship between the subfields of a finite field.

Since $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$, it is Galois over $\mathbb{F}_p$. As $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, the Galois group has order n. Though we showed this directly earlier, it immediately follows that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is generated by the Frobenius map $\phi(x) = x^p$, since the latter has order n. In other words

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}, \quad \phi^r \mapsto r.$$

If $d|n$, then the unique cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d is generated by k, where $n = dk$. That corresponds to the map $\phi^k(x) = x^{p^k}$. An element $\alpha \in \mathbb{F}_{p^n}$ is in the fixed field of $\langle \phi^k \rangle$ if and only if $\alpha^{p^k} = \alpha$, which is to say α is a root of $x^{p^k} - x$. Note that

$$k|n \Longrightarrow p^k - 1|p^n - 1 \Longrightarrow x^{p^k-1} - 1|x^{p^n-1} - 1 \Longrightarrow x^{p^k} - x|x^{p^n} - x$$

so the splitting field of $x^{p^n} - x$ contains the splitting field of $x^{p^k} - x$. It follows that

$$\mathbb{F}_{p^n}^{\langle \phi_k \rangle} = \mathbb{F}_{p^k}.$$

Then $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^k})$ is the subgroup of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ generated by ϕ^{p^k}, and isomorphic to $\mathbb{Z}/d\mathbb{Z}$.

Since $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is abelian, every subgroup is normal. Therefore $\mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p)$, which is isomorphic to $\langle \phi \rangle / \langle \phi^k \rangle \simeq (\mathbb{Z}/n\mathbb{Z})/(\mathbb{Z}/d\mathbb{Z}) \simeq \mathbb{Z}/k\mathbb{Z}$, is generated by the image of ϕ in the quotient.

To actually compute with a finite field $\mathbb{F}_q$, where $q = p^n$, we need to find a presentation with generators and relations. If $f(x)$ is an irreducible polynomial of degree n over $\mathbb{F}_p$, $\mathbb{F}_p[x]/(f(x))$ must be isomorphic to $\mathbb{F}_{p^n}$. Such irreducible polynomials do exist, but that requires a proof.

Proposition 13.1. *The finite field extensions $\mathbb{F}_{p^n}/\mathbb{F}_p$ are simple, i.e. $\mathbb{F}_{p^n} = \mathbb{F}_p[x]/(f(x))$ for some irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree n.*

Proof. This follows from the fact that $\mathbb{F}_{p^n}^\times$ is cyclic. Let α be a generator. Since every other element of $\mathbb{F}_{p^n}$ is a power of α, $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha] = \mathbb{F}_p[x]/(f(x))$, where $f(x) = m_\alpha(x)$ is the minimal polynomial of α over $\mathbb{F}_p$. As $\mathbb{F}_{p^n}$ has degree n over $\mathbb{F}_p$, so does $f(x)$. □

To find irreducible polynomials over $\mathbb{F}_p$, we use the following fact.

Proposition 13.2. *$x^{p^n} - x$ is the product of every distinct irreducible polynomials over $\mathbb{F}_p$ whose degree divides n.*

Proof. Let $f(x)$ be an irreducible polynomial of degree $d|n$. Then $\mathbb{F}_p[x]/(f(x)) \simeq \mathbb{F}_{p^d}$, which is isomorphic to a subfield of $\mathbb{F}_{p^n}$. Then $f(x)$ has a root in $\mathbb{F}_{p^n}$, and hence splits completely over it, since $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois. But then every root of $f(x)$, being an element of $\mathbb{F}_{p^n}$, is a root of $x^{p^n} - x$. Since $f(x)$ is separable, $f(x)|x^{p^n} - x$.

Conversely, suppose $f(x)$ is irreducible over $\mathbb{F}_p$, and divides $x^{p^n} - x$. Then its splitting field is contained in $\mathbb{F}_{p^n}$, and must be isomorphic to $\mathbb{F}_{p^d}$ for some $d|n$. On the other hand, since $\mathbb{F}_{p^d}$ is Galois, it must be isomorphic to $\mathbb{F}_p[x]/(f(x))$, hence $f(x)$ has degree d.

Since $x^{p^n} - x$ is separable, it's the product of all its distinct irreducible factors. □

Example 13.3. Over $\mathbb{F}_2$, we have

$$x^4 - x = x(x-1)(x^2 + x + 1),$$

Since there must exist an irreducible polynomial of degree 2 over $\mathbb{F}_2$, $x^2 + x + 1$ must be it.

Let α denote the image of x in $\mathbb{F}_2[x]/(x^2 + x + 1)$, so that

$$\mathbb{F}_4 = \mathbb{F}_2[\alpha] = \{0, 1, \alpha, \alpha + 1\}.$$

Note that

$$\alpha(\alpha + 1) = \alpha^2 + \alpha = -1 = 1, \quad (\alpha + 1)^2 = \alpha^2 + 1 = -\alpha = \alpha, \quad \alpha^2 = -\alpha - 1 = \alpha + 1.$$

Therefore the multiplication table of $\mathbb{F}_4^\times$ is

	1	α	$\alpha+1$
1	1	α	$\alpha+1$
α	α	$\alpha+1$	1
$\alpha+1$	$\alpha+1$	1	α

In a similar way, one can find a multiplication table for all $\mathbb{F}_{p^n}$ by factoring $x^{p^n}-x$ into irreducibles over $\mathbb{F}_p$, by choosing an irreducible $f(x)$ of degree n, and writing $\mathbb{F}_{p^n}=\mathbb{F}_p[x]/(f(x))$. The irreducible factors of $x^{p^n}-x$ of degree n are exactly the factors of degree n that aren't divisible by the irreducible factors of $x^{p^d}-x$ for $d|n$.

Example 13.4. Over $\mathbb{F}_3$ we have

$$x^9-x=x(x^8-1)=x(x^2-1)(x^4+x^2+1)=x(x-1)(x+1)(x^2+x+1)(x^2-x+1)$$

since

$$(x^2-x+1)(x^2+x+1)=(x^2+1)^2-x^2=x^4+2x^2+1-x^2=x^4+x^2+1.$$

Then $\mathbb{F}_3[x]/(x^2+x+1)\simeq\mathbb{F}_9$.

Now for $\mathbb{F}_{3^4}$ we have

$$x^{81}-x=x(x^{80}-1)=x(x^8-1)(x^{72}+x^{64}+x^{56}+\cdots+x^8+1).$$

The third factor is simply $f(x^8)$, for

$$f(x)=x^9+x^8+\cdots+x+1=(x^5+1)(x^4+x^3+x^2+x+1).$$

Then $x^8+1|x^{81}-x$ since $x+1|x^5+1|f(x)$. Now x^8+1 must be reducible over $\mathbb{F}_3$, since $\mathbb{F}_{3^8}\not\subseteq\mathbb{F}_{3^4}$. Indeed

$$(x^4+x^2-1)(x^4-x^2-1)=(x^4-1)^2-x^4=x^8-3x^4+1=x^8+1.$$

Over $\mathbb{F}_3$ we have

$$x^4+x^2-1=(x^2+x+1)(x^2-x+1)+1$$

so x^4+x^2-1 is not divisible by either of the irreducible quadratics over $\mathbb{F}_3$. It has no cubic factor, since $\mathbb{F}_{3^3}\not\subseteq\mathbb{F}_{3^4}$, so it must be irreducible. Therefore

$$\mathbb{F}_{81}=\mathbb{F}_3[x]/(x^4+x^2-1).$$

Although an 80×80 multiplication table for $\mathbb{F}_{81}^\times$ is too large to compute by hand, the above shows that each element of $\mathbb{F}_{81}$ can be written uniquely as $a\alpha^3+b\alpha^2+c\alpha+d$, where α is a root of x^4+x^2-1, and $a,b,c,d\in\{0,1,-1\}$. Writing the product of two such elements in the same form amounts to computing the residue of a polynomial of degree at most six modulo x^4+x^2-1.

Any two finite fields $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$ of characteristic p, for arbitrary m and n are contained in $\mathbb{F}_{p^{mn}}$. Then it's possible to take the "union" (really direct limit) of all such fields, and obtain

$$\overline{\mathbb{F}}_p=\cup_n\mathbb{F}_{p^n},$$

which is an algebraic closure of $\mathbb{F}_p$.

Finally, let us prove a classical result about the number of irreducible polynomials of a given degree modulo p. For this, we define the Möbius μ-function

$$\mu(n)=\begin{cases}1 & \text{if } n=1,\\ 0 & \text{if } n \text{ has a square factor},\\ (-1)^r & \text{if } n \text{ has } r \text{ distinct factors.}\end{cases}$$

and recall a result from elementary number theory, that if $f:\mathbb{N}\to\mathbb{C}$ is a function defined on the natural numbers, it has a *Möbius transform*

$$g(n)=\sum_{d|n}f(d)$$

which satisfies a *Möbius inversion formula*

$$f(n)=\sum_{d|n}\mu(d)g(\frac{n}{d}).$$

Proposition 13.5. *The number of distinct irreducibles of degree n over $\mathbb{F}_p$ is given by*

$$\frac{1}{n}\sum_{d|n}\mu(d)p^{n/d}$$

Proof. Let $f(n)$ be the number in question. Since the distinct irreducibles of degree $d|n$ are all the factors of $x^{p^n}-x$, counting degrees we get

$$p^n=\sum_{d|n}df(d).$$

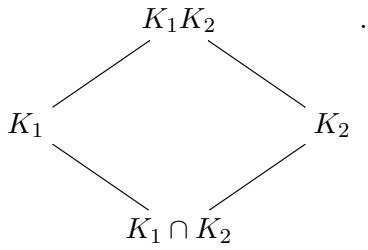
Then applying the Möbius inversion formula to $g(n)=p^n$ we obtain

$$nf(n)=\sum_{d|n}\mu(d)p^{n/d}.$$

□

14. Composite Extensions, Primitive Element Theorem

Given two subfields K_1 and K_2 of a larger field L, we may form the intersection $K_1\cap K_2$ as well as the composite field K_1K_2, both subfields of L. There is then a diagram



Proposition 14.1. *If $K_1/K_1\cap K_2$ is Galois, so is K_1K_2/K_2, and there is an isomorphism*

$$\mathrm{Gal}(K_1K_2/K_2)\xrightarrow{\sim}\mathrm{Gal}(K_1/K_1\cap K_2)$$

induced by restricting $\sigma\in\mathrm{Aut}(K_1K_2)$ to $\sigma|_{K_1}\in\mathrm{Hom}(K_1,K_2)$. In particular,

$$[K_1:K_1\cap K_2]=[K_1K_2:K_2].$$

Proof. Let $F=K_1\cap K_2$ and $K=K_1K_2$ for ease of notation. If K_1/F is Galois, K_1 is the splitting field of a separable $f(x)\in F[x]$. Then K_1K_2 is the splitting field of $f(x)\in K_2[x]$. Indeed, the splitting field of $f(x)$ over K_2 contains F and the roots of $f(x)$, so it contains K_1, hence also $K=K_1K_2$. Conversely, K_1K_2 contains K_1, hence the roots of $f(x)$, therefore also the splitting field of $f(x)$ over K_2. This shows K is Galois over K_2.

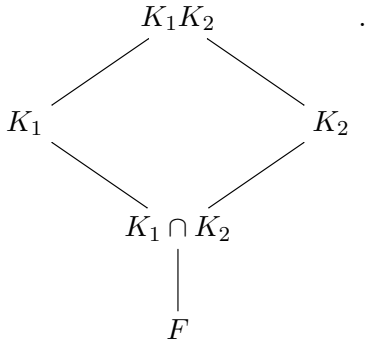
If α is a root of $f(x)$, since K_1/F is Galois, $K_1=F(\alpha)$, so that $[K_1:F]=\deg f$. Then $K=K_2(\alpha)$, and $[K:K_2]=\deg g$, where $g(x)$ is the minimal polynomial of α over K_2. In particular, $g(x)|f(x)$, and $[K:K_2]\leq[K_1:F]$.

Let $\sigma\in\mathrm{Gal}(K/K_2)$. Then $\sigma|_{K_1}$ is *a priori* an embedding of K_1 into K. Since $\sigma|_{K_2}=\mathrm{id}$, and $F\subset K_2$, $\sigma|_F=\mathrm{id}$, so that $\sigma|_{K_1}\in\mathrm{Hom}_F(K_1,K)$. Now since K_1/F is Galois, it follows that the inclusion $\mathrm{Aut}_F(K_1)\subset\mathrm{Hom}_F(K_1,K)$ is an equality, so that the map

$$\mathrm{Gal}(K/K_2)\to\mathrm{Gal}(K_1/F),\quad\sigma\mapsto\sigma|_{K_1}$$

is a well-defined group homomorphism. Let σ be in the kernel, so that $\sigma|_{K_1}=\mathrm{id}$. By definition of $\mathrm{Gal}(K/K_2)$ also $\sigma|_{K_2}=\mathrm{id}$, therefore $\sigma|_{K_1K_2}=\sigma=\mathrm{id}$. In other word, the map above is injective. Let $H\subset\mathrm{Gal}(K_1/F)$ be the image, and K_1^H its fixed field inside K_1. Now $K^{\mathrm{Gal}(K/K_2)}=K_2$, so that $K_1^{\mathrm{Gal}(K/K_2)}=K_1^H\subset K_2$. Then $F\subset K_1^H\subset K_1\cap K_2=F$, hence $K_1^H=F$, which shows $H=\mathrm{Gal}(K_1/F)$, therefore the map above is also surjective, hence an isomorphism. □

Now suppose K_1 and K_2 are both extensions of F, both contained in a larger field L. Again if K_1 is Galois over F, so is $K = K_1K_2$ over K_2. But now $K_1 \cap K_2$ may be larger than F, so we have



Corollary 14.2. *In the situation above, we have*

$$[K_1K_2 : F] = \frac{[K_1 : F][K_2 : F]}{[K_1 \cap K_2 : F]}.$$

Proof.

$$\frac{[K_1 : F][K_2 : F]}{[K_1 \cap K_2 : F]} = [K_1 : K_1 \cap K_2][K_2 : F] = [K_1K_2 : K_2][K_2 : F] = [K_1K_2 : F].$$

□

If both K_1 and K_2 are Galois over F, we may say more.

Proposition 14.3. *If K_1/F and K_2/F are Galois, so are K_1K_2/F and $K_1 \cap K_2/F$. Furthermore, the map*

$$\phi : \mathrm{Gal}(K_1K_2/F) \to \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F), \quad \sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$$

is injective with image

$$H = \{(\tau_1, \tau_2) : \tau_1|_{K_1 \cap K_2} = \tau_2|_{K_1 \cap K_2}\}$$

Proof. Let K_1/F and K_2/F be the fixed fields of H_1, H_2 in $\mathrm{Gal}(L/F)$, where L is a Galois extension of F containing K_1K_2. Assume K_1, K_2 are Galois over F, which is equivalent to H_1, H_2 being normal. Then $H_1 \cap H_2$ and $\langle H_1, H_2 \rangle$ are also normal, and their fixed fields are K_1K_2 and $K_1 \cap K_2$, which are therefore Galois over F.

The map ϕ is injective, since if $\sigma \in \mathrm{Aut}(K_1K_2/F)$ is identity on K_1 and K_2, it's also the identity on the field they generate. Note the image of ϕ is contained in H. We show it is in fact all of H by counting elements. Each $\tau_1 \in \mathrm{Gal}(K_1/F)$ occurs in some pair $(\tau_1, \tau_2) \in H$, since $\mathrm{Gal}(K_1K_2/F) \to \mathrm{Gal}(K_1/F)$ is surjective. If $(\tau_1, \tau_2) \in H$, then $(\tau_1, \tau_2') \in H$ if and only if

$$\tau_2|_{K_1 \cap K_2} = \tau_2'|_{K_1 \cap K_2} \iff \tau_2^{-1}\tau_2'|_{K_1 \cap K_2} = \mathrm{id} \iff \tau_2^{-1}\tau_2' \in \mathrm{Gal}(K_2/K_1 \cap K_2).$$

So the number of pairs $(\sigma, \sigma') \in H$ with $\sigma = \tau_1$ is equal to $|\mathrm{Gal}(K_2/K_1 \cap K_2)|$. Therefore by Proposition 14.1, the number of elements in H is equal to

$$|\mathrm{Gal}(K_1/F)| \cdot |\mathrm{Gal}(K_2/K_1 \cap K_2)| = [K_1 : F][K_1K_2 : K_1] = [K_1K_2 : F] = |\mathrm{Gal}(K_1K_2/F)|.$$

Then H has as many elements as the image of ϕ, hence must coincide with it. □

Corollary 14.4. *If K_1, K_2 are Galois over F, and $K_1 \cap K_2 = F$, then*

$$\mathrm{Gal}(K_1K_2/F) \to \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F), \quad \sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$$

is an isomorphism.

Proof. Immediate. □

Let K/F be a finite separable extension in some algebraic closure $\overline{K}$ of K. Then K is contained in some field L that is Galois over F. Indeed, if K is generated by $\alpha_1, \cdots, \alpha_r$ over F, and each α_i is the root of some irreducible $f_i(x)$ over F, then each $f_i(x)$ is separable, with a splitting field L_i that is Galois over F. The field L generated by L_i over F is then Galois by the proposition, and contains K.

If L' is another Galois extension of F containing K, by the Proposition so is $L' \cap L$.

Definition 14.5. The *Galois closure* L of K/F in $\overline{K}$ is the intersection of all Galois extensions of F containing K.

By construction, L/F is the minimal Galois extension containing K. When studying a finite extension K/F, it is often convenient to consider K as the subfield of its Galois closure.

Another convenience when dealing with arbitrary finite extensions K/F, is the assumption that K is *simple*, that is, $K = F(\alpha)$ for some α, whenever that is possible. If F is finite, we have seen that this is always the case. For infinite fields F, there is a general criterion for when a finite extension K/F is simple.

Proposition 14.6. *Let F be an infinite field, and K/F a finite extension. Then K is simple if and only if K has finitely many subfields.*

Proof. Assume $K = F(\alpha)$. If $f(x)$ is the minimal polynomial of α over F, then K is the splitting field of $f(x)$. Suppose L/F is a subfield of K. Then $K = L(\alpha)$. Let $g(x)$ be the minimal polynomial of α over L. Then $g(x)$ divides $f(x)$, so there are finitely many possibilities for it. On the other hand we claim $g(x)$ completely determines L.

Let L' be the subfield of L generated by the coefficients of $g(x)$. Then $g(x) \in L'[x]$ and $g(x)$ is irreducible over L' since it is so over L. Now on the one hand, since K/L is Galois, K is obtained by adjoining a root of $g(x)$ to L, hence $[K : L] = \deg g(x)$. On the other hand, the same is true for L', so $[K : L'] = \deg g(x)$. It follows that $[L : L'] = 1$ and $L = L'$.

Then L is determined by $g(x)$, and $g(x)|f(x)$. As there are finitely many (non-constant) polynomials that divide $f(x)$, there are finitely many subfields L of K.

Now conversely suppose F is infinite and K/F is a finite extension with finitely many subfields. Then $K = F(\alpha_1, \cdots, \alpha_r)$ for some $\alpha_i \in K$. To show K/F is simple it's enough to prove that for any $\alpha, \beta \in K$, $F(\alpha, \beta) = F(\gamma)$ for some other $\gamma \in K$. It would then follow by induction on r that K is simple.

Consider the extensions $F(\alpha + r\beta)$ as r varies in F. Since F is infinite, there are infinitely many such fields. Since K/F has finitely many subextensions, it must be the case that $F(\alpha + r\beta) = F(\alpha + r'\beta)$ for some pair of distinct r, $r' \in F$. Let $\gamma = \alpha + r\beta$. Then $F(\gamma) \subset F(\alpha, \beta)$. On the other hand

$$(\alpha+r\beta)-(\alpha+r'\beta) = (r-r')\beta \in F(\gamma) \Longrightarrow \beta \in F(\gamma) \Longrightarrow \alpha = (\alpha+r\beta)-r\beta \in F(\gamma) \Longrightarrow F(\alpha, \beta) \subset F(\gamma)$$

so that $F(\alpha, \beta) = F(\gamma)$. □

The proposition is usually employed in the following context.

Theorem 14.7. *Any finite separable extension K/F is simple. In particular, any finite extensions of a perfect field is simple.*

Proof. Let K/F be a finite separable extension. Then K has a Galois closure L/F, and any subfield K_0/F corresponds to some subgroup of $\mathrm{Gal}(L/F)$, of which there are finitely many. □

In particular, any finite extension of $\mathbb{Q}$ is simple.

Example 14.8. The extension $K = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$ must be simple. Let $\alpha = \zeta_3 + \sqrt[3]{2}$. Then

$$2 = (\alpha - \zeta_3)^3 = \alpha^3 - 3\alpha^2\zeta_3 + 3\alpha\zeta_3^2 - 1 = \alpha^3 - (3\alpha^2 + 3\alpha)\zeta_3 - 3\alpha - 1.$$

so

$$\zeta_3 = \frac{3-\alpha^3+3\alpha}{3\alpha^2+3\alpha} \in \mathbb{Q}(\alpha) \Longrightarrow \sqrt[3]{2} = \alpha - \zeta_3 \in \mathbb{Q}(\alpha) \Longrightarrow \mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \mathbb{Q}(\zeta_3 + \sqrt[3]{2}).$$

15. Cyclotomy

Using Galois Theory we can now carry out a more in-depth analysis of cyclotomic fields $\mathbb{Q}(\zeta_n)$. For each n, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois, since it's the splitting field of $x^n - 1$.

For each integer a coprime to n, the map σ_a defined by

$$\sigma_a|_{\mathbb{Q}} = \mathrm{id}, \quad \sigma_a(\zeta_n) = \zeta_n^a$$

defines an automorphism of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. This follows from the theorem on extension of isomorphisms, using the fact that ζ_n and ζ_n^a are both roots of the cyclotomic polynomial Φ_n, which is irreducible.

On the other hand, any such automorphism is fully determined by its value on ζ_n, since ζ_n generates $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$. We have therefore shown:

Proposition 15.1. *$\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois, and the map*

$$(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}), \quad a \mapsto \sigma_a$$

is an isomorphism.

□

Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. The elements

$$\{\zeta_n^a : 1 \le a \le n, \quad (a,n) = 1\} = \{\tau\zeta_n : \tau \in G\}$$

form a $\mathbb{Q}$-basis for $\mathbb{Q}(\zeta_n)$. Let H be a subgroup of G. Put

$$\alpha_H = \sum_{\sigma \in H} \sigma\zeta_n.$$

Proposition 15.2. $\mathbb{Q}(\zeta_n)^H = \mathbb{Q}(\alpha_H)$.

Proof. For each $\tau \in H$, we have $\tau H = \tau$, from which it follows that $\mathbb{Q}(\alpha_H) \subset \mathbb{Q}(\zeta_n)^H$, and so $H \subset \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\alpha_H))$. On the other hand, suppose that $\tau\alpha_H = \alpha_H$ for some $\tau \in G$. Then

$$\sum_{\sigma \in H} \tau\sigma\zeta_n = \sum_{\sigma \in H} \sigma\zeta_n.$$

Since the $\tau\zeta_n$ are linearly independent, the same elements must occur in the two sums above. In particular, $\tau\sigma\zeta_n = \zeta_n$ for some $\sigma \in H$. That implies $\tau\sigma = \mathrm{id}$, so $\tau = \sigma^{-1} \in H$. Therefore $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\alpha_H)) \subset H$. □

Example 15.3. The Galois group of $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ is cyclic of order 4, generated by $\sigma : \zeta_5 \to \zeta_5^3$. The unique subgroup of order 2 is generated by σ^2. Since $\sigma^2(\zeta_5) = \zeta_5^{-1}$ the corresponding subfield is $\mathbb{Q}(\zeta_5 + \zeta_5^{-1})$.

Example 15.4. The Galois group of $\mathbb{Q}(\zeta_{17})/\mathbb{Q}$ is cyclic of order 16, also generated by $\sigma : \zeta_{17} \mapsto \zeta_{17}^3$, since 3 is a generator of $(\mathbb{Z}/17\mathbb{Z})^\times$. Then $\langle\sigma^2\rangle$ is a cyclic subgroup of order 8, corresponding to the subfield $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta_n)$, where

$$\alpha = \sum_{k=0}^{7} \zeta_{17}^{9^k} = \zeta_{17} + \zeta_{17}^9 + \zeta_{17}^{13} + \zeta_{17}^{15} + \zeta_{17}^{16} + \zeta_{17}^8 + \zeta_{17}^4 + \zeta_{17}^2.$$

By Galois theory we know that $\mathbb{Q}(\alpha)$ is quadratic over $\mathbb{Q}$. In fact it is $\mathbb{Q}(\sqrt{17})$.

The sums $\sum_{\sigma\in H}\sigma\zeta_n$ are called *Gaussian periods*. One can show that for p an odd prime, the quadratic subextension of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is either $\mathbb{Q}(\sqrt{p})$ or $\mathbb{Q}(\sqrt{-p})$ according as whether p is 3 (mod 4) or 1 (mod 4). It follows that any quadratic extension $\mathbb{Q}(\sqrt{D})$ of $\mathbb{Q}$ is contained in some cyclotomic field. It turns out that much more is true.

Proposition 15.5. *For any finite abelian group G, there exists a field K contained in some cyclotomic field $\mathbb{Q}(\zeta_n)$ such that* $\mathrm{Gal}(K/\mathbb{Q})\simeq G$.

Proof. We know that every finite abelian group is a product of finite cyclic groups. Recall that if K_1, K_2 are Galois extensions of $\mathbb{Q}$ such that $K_1\cap K_2=\mathbb{Q}$, then $\mathrm{Gal}(K_1/\mathbb{Q})\times\mathrm{Gal}(K_2/\mathbb{Q})\simeq\mathrm{Gal}(K_1K_2/\mathbb{Q})$.

Suppose $G=H_1\times\cdots\times H_r$ where H_i are cyclic groups of orders n_i. Let p_i be distinct primes, congruent to 1 mod n_i. Then $(\mathbb{Z}/p_i\mathbb{Z})^\times$ has a subgroup of index n_i, corresponding to the subfield K_i of $\mathbb{Q}(\zeta_{p_i})$ such that $\mathrm{Gal}(K_i/\mathbb{Q})\simeq H_i$. Now for $i\neq j$ we have $\mathbb{Q}(\zeta_{p_i})\cap\mathbb{Q}(\zeta_{p_j})=\mathbb{Q}$. That follows, for instance, from the fundamental theorem of Galois theory, and the fact that $(\mathbb{Z}/p_ip_j\mathbb{Z})^\times$ is generated by the subgroups $(\mathbb{Z}/p_i\mathbb{Z})^\times$ and $(\mathbb{Z}/p_j\mathbb{Z})^\times$. Indeed, the subgroup generated by the two groups corresponds to the intersection of $\mathbb{Q}(\zeta_{p_i})$ and $\mathbb{Q}(\zeta_{p_j})$ in $\mathbb{Q}(\zeta_{p_ip_j})$. It follows that the subgroup of $\mathbb{Q}(\zeta_{p_1\cdots p_r})$ generated by $\mathbb{Q}(\zeta_{p_i})$ has Galois group isomorphic to the product of H_i, as desired. □

Definition 15.6. An *abelian extension* K of $\mathbb{Q}$, is a Galois extension whose group $\mathrm{Gal}(K/\mathbb{Q})$ is abelian.

We have shown that any finite abelian group is the Galois group of some subfield of a cyclotomic group. Let us quote the following remarkable theorem.

Theorem 15.7 (Kronecker-Weber)**.** *Any finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.*

The theorem says that abelian extensions are *the same* as subfields of cyclotomic fields. In other words, the field generated by all roots of unity over $\mathbb{Q}$ is the *maximal abelian extension* of $\mathbb{Q}$. The proof of this theorem is well outside the scope of this course, but it is one of the celebrated achievements of algebraic number theory.

We mention one last application of cyclotomy to a classical problem.

Proposition 15.8. *The regular n-gon is constructible with a ruler and compass if and only if n is a power of two times a product of distinct Fermat primes.*

Proof. To construct the regular n-gon with a ruler and compass amounts to constructing the point $(\cos(2\pi/n),\sin(2\pi/n))$ on the plane, in other words to construct ζ_n. We know that this is possible if and only if ζ_n lies in a tower of quadratic extensions

$$K_0=\mathbb{Q}\subset K_1\subset K_2\subset\cdots K_m.$$

It is a special case of a homework problem to show that any field K_m of degree a power of two over $\mathbb{Q}$ has such a tower of subfields. Then ζ_n is constructible if and only if it has degree 2^k over $\mathbb{Q}$. Now if $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$, then

$$\varphi(n)=\prod_i(p_i^{\alpha_i}-p_i^{\alpha_i-1}).$$

Thus $\varphi(n)$ is a power of two if and only if each $p_i^{\alpha_i}-p_i^{\alpha_i-1}$ is a power of two. If $\alpha_i>1$ for some i, then $p|p_i^{\alpha_i}-p_i^{\alpha_i-1}$, hence $p=2$. If $\alpha_i=1$, then $p-1$ must be a power of two, hence a Fermat prime. Conversely, if $n=2^kp_1\cdots p_r$ where $p_i=2^{n_i}+1$, then $\varphi(n)=2^{n_1+\cdots n_r+k-1}$. □

16. Applications of Galois Theory

Let K/F be a finite Galois extension. We have seen that K must be the splitting field of a polynomial $f(x) \in F[x]$.

Assume $f(x)$ is irreducible, with roots $\alpha_1, \cdots, \alpha_n$. An element $\sigma \in \mathrm{Gal}(K/F)$ is completely determined by its action on the roots α_i. This gives an injection $\mathrm{Gal}(K/F) \hookrightarrow S_n$, where S_n is the symmetric group of n elements.

A subgroup G of S_n is called *transitive* if for any $i, j \in \{1, \cdots, n\}$, $i \neq j$, there exists $\sigma \in G$ such that $\sigma(i) = j$. Galois groups are transitive subgroups of S_n, because $F(\alpha_i)$ is isomorphic to $F(\alpha_j)$, and any such isomorphism may be extended to an element of $\mathrm{Gal}(K/F)$.

If $f(x)$ factors into $f_1(x) \cdots f_r(x)$, and each $f_i(x)$ has degree n_i, then the Galois group of $f(x)$ injects into $S_{n_1} \times \cdots \times S_{n_r}$, and the projection of its image onto each S_{n_i} is a transitive subgroup. We still don't know exactly *which* transitive subgroups can appear as Galois group of a polynomial.

Open Problem. Which finite groups appear as Galois groups of rational polynomials? This is called the *inverse Galois problem.*

We won't say more about this, and instead turn to an application of Galois theory to rational functions.

Symmetric Rational Functions

Let F be a field, and $x_1, \cdots, x_n$ variables.

Definition 16.1. The *elementary symmetric functions* in $x_1, \cdots, x_n$ are

$$\begin{aligned}
s_1 &= x_1 + \cdots + x_n \\
s_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = \prod_{1 \leq i < j \leq n} x_i x_j \\
s_3 &= x_1x_2x_3 + \cdots x_{n-2}x_{n-1}x_n = \prod_{1 \leq i < j < k \leq n} x_i x_j x_k \\
&\vdots \\
s_n &= x_1x_2 \cdots x_n
\end{aligned}$$

The field $F(s_1, \cdots, s_n)$ generated by s_i is a subfield of $F(x_1, \cdots, x_n)$, the field of rational functions in x_i. Note that s_n are the coefficients of a polynomial with roots x_n:

$$p(x) = (x - x_1)(x - x_2) \cdots (x - x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n.$$

Then $F(x_1, \cdots, x_n)$ is the splitting field of $p(x) \in F(s_1, \cdots, s_n)$. Therefore $F(x_1, \cdots, x_n)$ is Galois over $F(s_1, \cdots, s_n)$, and the Galois group has at most $n!$ elements.

For any $\sigma \in S_n$, define an automorphism of $F(x_1, \cdots, x_n)$, also called σ, as follows. If $\sigma(i) = j$, then put $\sigma(x_i) = x_j$. This defines an automorphism of $F[x_1, \cdots, x_n]$, hence also one of $F(x_1, \cdots, x_n)$. We have thus shown:

Proposition 16.2. *The Galois group of $F(x_1, \cdots, x_n)/F(s_1, \cdots, s_n)$ is S_n.*

Corollary 16.3. *Any rational function in $x_1, \cdots, x_n$ that is invariant under permutations of x_i may be written as a function of $s_1, \cdots, s_n$.*

Example 16.4. Consider $f(x) = x_1^3 + x_2^3 + x_3^3$. It is an element of $F(x_1, x_2, x_3)$, and invariant under permutations of x_1, x_2, x_3. Then $f(x)$ must be a function of s_1, s_2, s_3. Indeed we have

$$\begin{aligned} f(x) &= (x_1+x_2+x_3)^3 - 3x_1^2x_2 - 3x_2^2x_1 - 3x_2^2x_3 - 3x_2x_3^2 - 3x_1x_3^2 - 3x_2^2x_3 - 6x_1x_2x_3 \\ &= (x_1+x_2+x_3)^3 - 3x_1x_2(x_1+x_2+x_3) - 3x_1x_3(x_1+x_2+x_3) - 3x_2x_3(x_1+x_2+x_3) + 3x_1x_2x_3 \\ &= s_1^3 - 3s_1s_2 + 3s_3. \end{aligned}$$

One may also start with $s_1, \cdots, s_n$ are indeterminates, and define

$$p(x) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n.$$

The roots of $p(x)$ are, as a set, determined by $s_1, \cdots, s_n$. They may *a priori* have algebraic relations between themselves. However:

Lemma 16.5. *The roots $x_1, \cdots, x_n$ of $p(x)$ are algebraically independent. In other words if $p(y_1, \cdots, y_n) \in F[y_1, \cdots, y_n]$ is any non-zero polynomial, $p(x_1, \cdots, x_n) \neq 0$.*

Proof. Assume $p(x_1, \cdots, x_n) = 0$. Then for

$$q(y_1, \cdots, y_n) = \prod_{\sigma \in S_n} p(y_{\sigma(1)}, \cdots, y_{\sigma(n)}),$$

we have $q(x_1, \cdots, x_n) = 0$. By construction, $q(y_1, \cdots, y_n)$ is invariant under permutations of y_i. That implies $q(x_1, \cdots, x_n) = f(s_1, \cdots, s_n)$ for some polynomial f. But $f(s_1, \cdots, s_n) \neq 0$, since the s_i are indeterminates. □

Corollary 16.6. *$p(x)$ is a separable polynomial over $F(s_1, \cdots, s_n)$ with Galois group S_n.*

One way to interpret this statement is to say that the *generic* polynomial $p(x_1, \cdots, x_n)$ has Galois group S_n. There is some sense in which this is true for *most* polynomials over $\mathbb{Q}$. In a precise asymptotic sense the proportion of polynomials of degree n with Galois group S_n approaches 1.

The precise statement is as follows, stated without proof.

Theorem 16.7 (P.X. Gallagher)**.** *Let $R_n(M)$ denote the number of polynomials of degree n with coefficients $|a_i| \leq M$ and Galois group not equal to S_n. Then*

$$|R_n(m)| \ll M^{n-1/2} \log M.$$

Definition 16.8. The *discriminant* of a set of numbers $x_1, \cdots, x_n$ is

$$D = \prod_{i<j} (x_i - x_j)^2.$$

The discriminant of a polynomial is the discriminant of its roots.

It's easy to see that D is invariant under transpositions, hence under all elements of S_n. Therefore D is a function of $s_1, \cdots, s_n$.

If $n \geq 5$, A_n is the only normal subgroup of S_n, and it has index 2. It corresponds to a subfield of $F(x_1, \cdots, x_n)$ of degree 2 over $F(s_1, \cdots, s_n)$. Note that $\sigma \in A_n$ if and only if σ fixes

$$\sqrt{D} = \prod_{i<j} (x_i - x_j)$$

If $\mathrm{char}(F) \neq 2$, then $F(s_1, \cdots, s_n, \sqrt{D})$ is quadratic and Galois over $F(s_1, \cdots, s_n)$, hence corresponds to $A_n \subset S_n$.

Fundamental Theorem of Algebra

The fundamental theorem of algebra in fact is not entirely algebraic, since it concerns the complex numbers, which are analytic in nature. We may use Galois theory to give a quick proof, using the following facts:

(a) Any odd-degree polynomial with real coefficients has a real root.
(b) Any quadratic polynomial over the complex numbers has a complex root.

Fact (a) is a consequence of the intermediate value theorem from calculus. This is the inevitable analytic input. Fact (b) is however algebraic: it follows from the quadratic formula, which may be derived by completing the square.

Theorem 16.9. *Any non-constant polynomial $p(x) \in \mathbb{C}[x]$ has a root in $\mathbb{C}$. In other words, $\mathbb{C}$ is algebraically closed.*

Proof. First we show that it's enough to prove this for $p(x) \in \mathbb{R}[x]$. Indeed, $p(x)$ has a complex root if and only if $\overline{p}(x)$ does, which is the polynomial obtained from $p(x)$ by complex conjugation. Then $p(x)$ has a complex root if and only if $q(x) = \overline{p}(x)p(x)$ does. Now $q(x)$ is invariant under complex conjugation, hence it belongs to $\mathbb{R}[x]$.

Now, let $p(x) \in \mathbb{R}[x]$ be non-constant, and $K/\mathbb{R}$ its splitting field. Let H be the Sylow-2 subgroup of $\mathrm{Gal}(K(i)/\mathbb{R})$. Then $K(i)^H$ has odd degree over $\mathbb{R}$. By fact (a), $K(i)^H$ must be the trivial extension, i.e. $\mathbb{R}$ itself. Therefore $\mathrm{Gal}(K(i)/\mathbb{R})$ is a finite 2-group, and hence so is $\mathrm{Gal}(K(i)/\mathbb{C})$, say of order 2^n. If $n \geq 1$, the latter must therefore contain a subgroup H' of order 2^{n-1}, of index 2 and necessarily normal. Then $K(i)^{H'}$ is a quadratic extension of $\mathbb{C}$. By fact (b) this is impossible, so $n = 0$, and $K(i) = \mathbb{C}$. In other words, $\mathbb{C}$ contains all the roots of $p(x)$. □

Solvability by Radicals

If $p(x)$ is a polynomial of degree 2, 3, or 4, the equation $p(x) = 0$ has a formulaic solution given by the quadratic, cubic, and quartic formulas. These formulas all involve the four basic operations, plus extraction of nth roots. We say $p(x) = 0$ is *solvable by radicals*. Abel's Theorem implies that there is no such general formula for $p(x)$ of degree ≥ 5. This is the theorem we wish to prove:

Theorem 16.10. *Let F be a field of characteristic 0. If $p(x) \in F[x]$ is a polynomial with Galois group G, then*

$$p(x) = 0$$

is solvable by radicals if and only if G is solvable.

Recall that a solvable group G is one that admits a sequence of normal subgroups

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G$$

such that G_i/G_{i-1} is cyclic.

Proposition 16.11. *Let F be a field containing the nth roots of unity, of characteristic not dividing n. Then for $a \in F$, $F(\sqrt[n]{a})$ is a cyclic Galois extension of F of degree dividing n.*

Proof. Note $\sqrt[n]{a}$ is a root of $x^n - a$, and all the other roots differ from $\sqrt[n]{a}$ by a power of ζ_n, which lies in F. $F(\sqrt[n]{a})$ is the splitting field of $x^n - a$ over F, and is therefore normal. Since $\mathrm{char}(F) \neq n$, $nx^{n-1} \neq 0$, therefore $x^n - a$ is also separable, and $K = F(\sqrt[n]{a})$ is Galois over F.

Let $\sigma \in \mathrm{Gal}(K/F)$, then $\sigma(\sqrt[n]{a}) = \zeta\sqrt[n]{a}$, where ζ is some nth root of unity. Define a map

$$\phi : \mathrm{Gal}(K/F) \to \mu_n, \quad \phi(\sigma) = \zeta.$$

It is injective, since K is generated by $\sqrt[n]{a}$. For $\sigma, \tau \in \mathrm{Gal}(K/F)$ we have

$$\sigma\tau(\sqrt[n]{a}) = \sigma(\phi(\tau)\sqrt[n]{a}) = \phi(\sigma)\phi(\tau)\sqrt[n]{a} \Longrightarrow \phi(\sigma\tau) = \phi(\sigma)\phi(\tau).$$

This shows ϕ is a group homomorphism. Therefore $\mathrm{Gal}(K/F)$ is isomorphic to a subgroup of μ_n, which is cyclic of order n. □

This proposition has a converse, for which we have to introduce a construction. As before, let F be a field of characteristic $\neq n$, containing μ_n. Let K/F be a cyclic extension of degree n, with Galois group generated by σ.

Definition 16.12. For $a \in K$, $\zeta \in \mu_n$, the *Lagrange resolvent* $(a, \zeta) \in K$ is defined as

$$(a, \zeta) = a + \zeta\sigma(a) + \zeta^2\sigma^2(a) + \cdots + \zeta^{n-1}\sigma^n.$$

Note that

$$\sigma((a, \zeta)) = \sigma(a) + \zeta\sigma^2(a) + \cdots + \zeta^{n-1}\sigma^n(a) = \zeta^{-1}(\zeta\sigma(a) + \cdots \zeta^{n-1}\sigma^{n-1}(a) + \zeta^n\sigma^n(a)) = \zeta^{-1}(a, \zeta).$$

Proposition 16.13. *Let F be a field containing μ_n of characteristic not dividing n. If K/F is a cyclic Galois extension, then $K = F(\sqrt[n]{a})$ for some $a \in F$.*

Proof. Let σ be a generator of $\mathrm{Gal}(K/F)$. We have

$$\sigma((a, \zeta)^n) = \zeta^{-n}(a, \zeta)^n = (a, \zeta)^n \implies (a, \zeta)^n \in F.$$

Since the characters $1, \sigma, \cdots, \sigma^{n-1}$ are linearly independent, there must exist some $a \in K$, such that $(a, \zeta) \neq 0$. Then

$$\sigma^k(a, \zeta) = \zeta^{-k}(a, \zeta) \neq (a, \zeta)$$

for any $k = 1, \cdots, n-1$. It follows that (a, ζ) is not fixed by any σ^k, and therefore not by any subgroup of $\mathrm{Gal}(K/F)$. Hence

$$K = F((a, \zeta)) = F(\sqrt[n]{b}),$$

where $b = (a, \zeta)^n$. □

From now on we assume F has characteristic 0. If $a \in F$, by $\sqrt[n]{a}$ we denote *any* root of $x^n - a$.

Definition 16.14. A finite extension K/F is a *root extension* if there exist subfields

$$K_0 = F \subset K_1 \subset K_2 \subset \cdots \subset K_n = K$$

such that $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for some $a_i \in K_i$, $i = 0, \cdots, n-1$.

If α is algebraic over F, we say it can be *expressed by radicals* if α lies in a root extension of F.

We say a polynomial $p(x) \in F[x]$ is *solvable by radicals* if all its roots lie in a root extension of F.

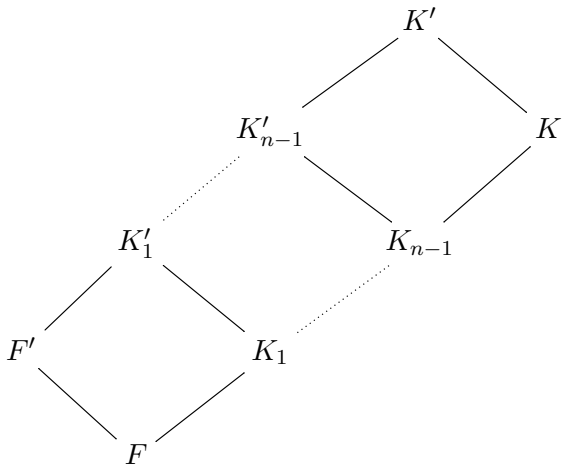
Elements of root extensions of F are exactly the numbers that have expressions like

$$\sqrt[a]{x + \sqrt[b]{y + \sqrt[c]{z}}} - \sqrt[d]{u - \sqrt[e]{v - \sqrt[f]{w}}}.$$

The roots of a polynomial $p(x) \in F[x]$ of degree 2, 3, or 4 have general expressions in terms of radicals. We want to show no such general formula is possible in degree 5 using Galois theory. To do that, our fields must be Galois.

Lemma 16.15. *Let K/F be a root extension so that there exist $F = K_0 \subset K_1 \subset \cdots \subset K_n = K$ such that $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for $a_i \in K_i$. Suppose $F' = F(\sqrt[n]{a})$ for some $a \in F$, and put $K' = KF'$. Then K'/F is a root extension.*

Proof. Let $K_i' = F'K_i$:



Then we have

$$F \subset F' \subset K_1' \subset K_2' \subset \cdots K_n' \subset K'$$

where $F' = F(\sqrt[n]{a})$ and $K'_{i+1} = K'_i(\sqrt[n_i]{a_i})$. □

Corollary 16.16. *If K/F and K'/F are root extensions, so is KK'/F.*

Proof. Suppose

$$F = K_0 \subset K_1 \subset \cdots K_n = K$$

and

$$F = K_0' \subset K_1' \subset \cdots K_n' = K'.$$

Applying the lemma inductively to the extensions K'_{i+1}/K_i we obtain that $K_1'K/F$, $K_2'K/F$, $\cdots$, $K_n'K/F$ are all root extensions. □

Corollary 16.17. *If K/F is a root extension, and L is a Galois closure of K, then L/F is a root extension.*

Proof. Given $\sigma \in \mathrm{Gal}(L/F)$, and $F = K_0 \subset K_1 \subset \cdots \subset K_n = K$ we have

$$F = \sigma K_0 \subset \sigma K_1 \subset \cdots \sigma K_n = \sigma K.$$

If $K_{i+1} = K_i(\sqrt[n_i]{a_i})$, then $\sigma K_{i+1} = \sigma K_i(\sigma \sqrt[n_i]{a_i})$. Since $\sqrt[n_i]{a_i}$ is a root of $x^{n_i} - a_i$, $\sigma(\sqrt[n_i]{a_i})$ is a root of $x^{n_i} - \sigma a_i$. Therefore if K/F is a root extension, so is $\sigma K/F$. If $\mathrm{Gal}(L/K) = \{\sigma_1, \cdots \sigma_r\}$, then applying the previous corollary inductively, the composite of all $\sigma_i K$, which is L, is a root extension of F. □

Proposition 16.18. *An algebraic number α over F lies in a root extension K/F if and only if it lies in a Galois extension L/F such that there exist L_i,*

$$F = L_0 \subset L_1 \subset L_1 \subset \cdots \subset L_n = K$$

where each L_{i+1}/L_i is Galois and cyclic.

Proof. Suppose $F = K_0 \subset K_1 \subset \cdots \subset K_n = K$ where $K_{i+1} = K_i(\sqrt[n_i]{a_i})$. If $F' = F(\zeta_{n_i})$ and $K_i' = F'K_i$, then $K'_{i+1} = K'_i(\sqrt[n_i]{a_i})$ is Galois and cyclic over K_i', being the splitting field of $x^{n_i} - a_i$. Extending the tower inductively in this way by adjoining ζ_{n_1}, ζ_{n_2}, $\cdots$, ζ_{n_r}, we obtain a tower where every successive extension is Galois and cyclic.

Conversely, suppose $\alpha \in L$, where L/F is as in the proposition. If L_{i+1}/L_i has order n_i, then again adjoining $\zeta_{n_1}, \zeta_{n_2}, \cdots, \zeta_{n_r}$ to the tower, each successive extension becomes of the form $L'_{i+1} = L'_i(\sqrt[m_i]{a_i})$, where $m_i | n_i$, by Proposition 16.13. □

Theorem 16.19 (Galois)**.** *A polynomial $p(x) \in F[x]$ is solvable by radicals if and only if the Galois group of $p(x)$ is solvable.*

Proof. Suppose the Galois group of $p(x)$ is solvable. If L is the splitting field, and $G = \mathrm{Gal}(L/F)$, there exist normal subgroups

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G,$$

such that G_{i+1}/G_i is cyclic. By the Galois correspondence G_{n-i} correspond to Galois extensions L_i/F such that

$$F = L_0 \subset L_1 \subset \cdots \subset L_n = L$$

where $G_{n-i} = \mathrm{Gal}(L_n/L_i)$. Then $\mathrm{Gal}(L_{i+1}/L_i) = \mathrm{Gal}(L/L_i)/\mathrm{Gal}(L/L_{i+1}) = G_{n-i}/G_{n-i-1}$ is cyclic. By the proposition each element of $\alpha \in L$ lies in a root extension, hence $p(x)$ is solvable by radicals.

Conversely, suppose $p(x)$ is solvable by radicals, and α is a root lying in a root extension K/F. By the proposition it lies in a solvable Galois extension L/F. As L is Galois, it must contain the splitting field K of $p(x)$. Then $\mathrm{Gal}(K/F)$ is a quotient of $\mathrm{Gal}(L/F)$, therefore it is solvable. □

Corollary 16.20. *The general polynomial $p(x)$ of degree $n \geq 5$ is not solvable by radicals.*

Proof. The Galois group of such a $p(x)$ is S_n, which is not solvable if $n \geq 5$. □

Let $p(x) \in \mathbb{Q}[x]$ be an irreducible quintic polynomial. The number of real roots of $p(x)$ is either 1, 3 or 5, since an irreducible polynomial over $\mathbb{R}$ must have even degree. We claim that if $p(x)$ has exactly 3 real roots, it is not solvable by radicals.

Let L be the splitting field of $p(x)$, and assume $L \subset \mathbb{C}$. Then $\mathrm{Gal}(L/\mathbb{Q})$ is a subgroup of S_5. Since L contains $K = F[x]/(p(x))$, and $[K : F] = 5$, $|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}]$ is divisible by 5. Then $\mathrm{Gal}(L/\mathbb{Q})$ has an elements of order 5, which must be a 5-cycle in S_5. Now, if $p(x)$ has exactly three real roots, complex conjugation on L switches the two complex roots, hence defines a transposition in $\mathrm{Gal}(L/\mathbb{Q})$. Then $\mathrm{Gal}(L/\mathbb{Q})$ must be S_5, since that is generated by any 5-cycle and transposition, and so $p(x)$ is not solvable by radicals.

Suppose $p(x)$ is monic. To show $p(x)$ has at least three real roots, by the intermediate value theorem it's enough to find $a, b \in \mathbb{R}$ such that $a < b$, $p(a) > 0$ and $p(b) < 0$. To show $p(x)$ has at most three real roots by the mean value theorem it's enough to show that $p'(x)$ does not have four distinct real roots.

Example 16.21. Consider $p(x) = x^5 - 4x^4 + 2 \in \mathbb{Q}[x]$. It is irreducible by Eisenstein's criterion. Since $p(0) = 2$ and $p(1) = -1$, it has at least three real roots. Since $p'(x) = 5x^4 - 16x^3$ has exactly two real roots, $p(x)$ can not have five (distinct) real roots, so it has three. Therefore the Galois group of $p(x)$ is S_5, and the roots of $p(x)$ can not be expressed in terms of radicals.

17. Solving polynomial Equations of degree 3 and 4

We apply Galois theory to derive Cardano's formula for the cubic and therefore put it in a more conceptual context.

Let $f(x) = x^3 + ax^2 + bx + c \in F = \mathbb{Q}(a, b, c)[x]$. To solve $f(x) = 0$, we may first make a simple substitution $g(x) = f(x - \frac{a}{3})$ to obtain

$$g(x) = x^3 + px + q$$

where

$$p = \frac{1}{3}(b - 3a^2), \quad q = \frac{1}{27}(2a^3 - 9ab + 27c).$$

Let α, β, γ be the roots of $g(x)$, and $\zeta = \zeta_3$. Then $K = F(\alpha, \beta, \gamma)$ is the splitting field of $f(x)$ over F, and the Galois group of K/F is S_3.

Recall that the discriminant of $g(x)$ is given by

$$D = (\alpha-\beta)^2(\beta-\gamma)^2(\alpha-\gamma)^2.$$

Taking the square root

$$\sqrt{D} = (\alpha-\beta)(\beta-\gamma)(\alpha-\gamma)$$

we have $F(\sqrt{D}) \subset K$. An element $\sigma \in S_3$ fixes $F(\sqrt{D})$ if and only if $\sigma \in A_3$. Therefore $\mathrm{Gal}(K/F(\sqrt{D})) \simeq A_3 = C_3$, a cyclic group of order 3.

Lagrange resolvents allow us to compute generators for cyclic extensions of order n, as long as the base field contains the nth roots of unity. Therefore we adjoint ζ to obtain $K(\zeta)/F(\sqrt{D},\zeta)$.

If σ is the generator of $\mathrm{Gal}(K/F)$, we can assume $\sigma\alpha = \beta$, and $\sigma\beta = \gamma$. Consider now the resolvents

$$\begin{aligned}(\alpha,1) &= \alpha + \sigma\alpha + \sigma^\alpha = \alpha+\beta+\gamma = 0,\\ \lambda_1 = (\alpha,\zeta) &= \alpha + \zeta\sigma\alpha + \zeta^2\sigma^2\alpha = \alpha+\zeta\beta+\zeta^2\gamma,\\ \lambda_2 = (\alpha,\zeta^2) &= \alpha + \zeta^2\sigma\alpha + \zeta\sigma^2\alpha = \alpha+\zeta^2\beta+\zeta\gamma.\end{aligned}$$

and note that

$$\lambda_1+\lambda_2 = 2\alpha-\beta-\gamma = 3\alpha, \quad \zeta^2\lambda_1+\zeta\lambda_2 = 3\beta$$

so it's enough to solve for λ_1, λ_2. We know that $\lambda_1^3, \lambda_2^3 \in F(\sqrt{D},\zeta)$. Writing:

$$\lambda_1^3 = (\alpha^3+\beta^3+\gamma^3) + 3\zeta(\alpha^2\beta+\beta^2\gamma+\gamma^2\alpha) + 3\zeta^2(\alpha\beta^2+\beta\gamma^2+\gamma\alpha^2) + 6\alpha\beta\gamma.$$

The first and last terms are invariant under $\mathrm{Gal}(K(\zeta)/\mathbb{Q}(\zeta)) \simeq S_3$ so must be expressible in terms of p and q. The middle two terms are invariant under cyclic permutations, so must be expressible in terms of $\sqrt{D}$, p, q, and ζ.

Using Example 16.4, since the symmetric polynomials in α, β, γ are

$$s_1 = \alpha+\beta+\gamma = 0, \quad s_2 = \alpha\beta+\alpha\gamma+\beta\gamma = p, \quad s_3 = \alpha\beta\gamma = -q,$$

we have

$$\alpha^3+\beta^3+\gamma^3 = s_1^3 - 3s_1s_2 + 3s_3 = -3q, \quad 6\alpha\beta\gamma = -6q.$$

To find the middle terms in terms of p, q and $\sqrt{D}$ we expand

$$\sqrt{D} = \alpha^2\beta+\beta^2\gamma+\gamma^2\alpha - (\beta^2\alpha+\gamma^2\beta+\alpha^2\gamma)$$

and see that

$$3\zeta(\alpha^2\beta+\beta^2\gamma+\gamma^2\alpha) = \frac{3}{2}\zeta(A+\sqrt{D}), \quad 3\zeta^2(\alpha\beta^2+\beta\gamma^2+\gamma\alpha^2) = \frac{3}{2}\zeta^2(A-\sqrt{D})$$

where

$$\begin{aligned}A &= \alpha^2\beta+\beta^2\gamma+\gamma^2\alpha + (\beta^2\alpha+\gamma^2\beta+\alpha^2\gamma)\\ &= \alpha\beta(\alpha+\beta)+\alpha\gamma(\alpha+\gamma)+\beta\gamma(\beta+\gamma)\\ &= -3\alpha\beta\gamma = 3q.\end{aligned}$$

The above is invariant under the action of S_3, so must be expressible in terms of p and q. Altogether

$$\lambda_1^3 = -3q + \frac{3}{2}\zeta(3q+\sqrt{D}) + \frac{3}{2}\zeta^2(3q-\sqrt{D}) - 6q$$

which using $\zeta+\zeta^2 = -1$ and $\zeta-\zeta^2 = \sqrt{-3}$ becomes

$$\lambda_1^3 = \frac{-27}{2}q - \frac{3}{2}\sqrt{-3D}.$$

If τ is the automorphism of $F(\zeta)$ that sends ζ to ζ^2, then $\tau(\lambda_1 = \lambda_2)$. It follows that λ_2^3 differs from λ_1^3 by replacing $\zeta - \zeta^2$ with $\zeta^2 - \zeta$, i.e.

$$\lambda_2^3 = \frac{-27}{2}q + \frac{3}{2}\sqrt{-3D}.$$

Then one must take cube roots to find λ_1, λ_2. The choice for λ_1 forces the one for λ_2, since

$$\lambda_1\lambda_2 = (\alpha + \zeta\beta + \zeta^2\gamma)(\alpha + \zeta^2\beta + \zeta\gamma) = \alpha^2 + \beta^2 + \gamma^2 - 3\alpha - 3\beta - 3\gamma = -3p.$$

With this compatible choice of cube roots we obtain Cardano's formula:

$$\alpha = \frac{1}{3}\left(\sqrt[3]{\frac{-27}{2}q - \frac{3}{2}\sqrt{-3D}} + \sqrt[3]{\frac{-27}{2}q + \frac{3}{2}\sqrt{-3D}}\right),$$

$$\beta = \frac{1}{3}\left(\zeta^2\sqrt[3]{\frac{-27}{2}q - \frac{3}{2}\sqrt{-3D}} + \zeta\sqrt[3]{\frac{-27}{2}q + \frac{3}{2}\sqrt{-3D}}\right),$$

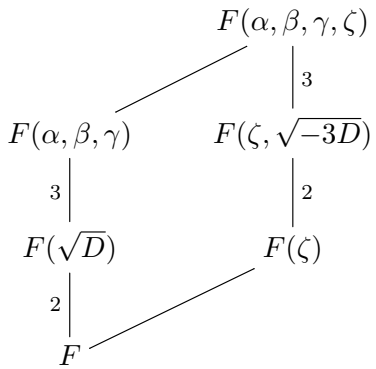
and

$$\gamma = \frac{1}{3}\left(\zeta\sqrt[3]{\frac{-27}{2}q - \frac{3}{2}\sqrt{-3D}} + \zeta^2\sqrt[3]{\frac{-27}{2}q + \frac{3}{2}\sqrt{-3D}}\right),$$

where

$$D = -4p^3 - 27q^2.$$

We can depict this process in the diagram



Since $F(\zeta, \sqrt{-3D})$ contains ζ, the upper-right field, which is cyclic over it, may be obtained by adjoining explicit cube roots using Lagrange resolvents.

Quartic Equations

Let $f(x) = x^4 + ax^3 + bx^2 + cx + d$ be an irreducible polynomial over $\mathbb{Q}$. As in the cubic case, we let $g(x) = f(x - \frac{a}{4}) = x^4 + px^2 + qx + r$, where p, q, r now have more complicated expressions:

$$\begin{aligned} p &= \frac{1}{8}(-3a^2 + 8b) \\ q &= \frac{1}{8}(a^3 - 4ab + 8c) \\ r &= \frac{1}{256}(-3a^4 + 16a^2b - 64ac + 256d). \end{aligned}$$

Now $g(x)$ is irreducible since $f(x)$ is, and solving $g(x) = 0$ is equivalent to solving $f(x) = 0$. Let $\alpha, \beta, \gamma, \delta$ be the roots of $g(x)$.

Let

$$\begin{aligned}\lambda_1 &= (\alpha+\beta)(\gamma+\delta)\\ \lambda_2 &= (\alpha+\gamma)(\beta+\delta)\\ \lambda_3 &= (\alpha+\delta)(\beta+\gamma)\end{aligned}$$

Since $\alpha+\beta+\gamma+\delta=0$, we have

$$\begin{aligned}\alpha+\beta &= \sqrt{-\lambda_1}, \quad \gamma+\delta = -\sqrt{-\lambda_1}\\ \alpha+\gamma &= \sqrt{-\lambda_2}, \quad \beta+\delta = -\sqrt{-\lambda_2}.\\ \alpha+\delta &= \sqrt{-\lambda_3}, \quad \beta+\gamma = -\sqrt{-\lambda_3}.\end{aligned}$$

Then since $\alpha+\beta+\gamma+\delta=0$, we have

$$\begin{aligned}\alpha &= \frac{1}{2}\left(\sqrt{-\lambda_1}+\sqrt{-\lambda_2}+\sqrt{-\lambda_3}\right),\\ \beta &= \frac{1}{2}\left(\sqrt{-\lambda_1}-\sqrt{-\lambda_2}-\sqrt{-\lambda_3}\right).\\ \gamma &= \frac{1}{2}\left(-\sqrt{-\lambda_1}+\sqrt{-\lambda_2}-\sqrt{-\lambda_3}\right),\\ \delta &= \frac{1}{2}\left(-\sqrt{-\lambda_1}-\sqrt{-\lambda_2}+\sqrt{-\lambda_3}\right).\end{aligned}$$

We have

$$\begin{aligned}(\alpha+\beta)(\alpha+\gamma)(\alpha+\delta) &= (\alpha^2+\alpha\gamma+\beta\gamma+\alpha\beta)(\alpha+\delta)\\ &= \alpha^3+\alpha^2\gamma+\alpha\beta\gamma+\alpha^2\beta+\alpha^2\delta+\alpha\gamma\delta+\beta\gamma\delta+\alpha\beta\delta\\ &= \alpha^2(\alpha+\beta+\gamma+\delta)-q = -q.\end{aligned}$$

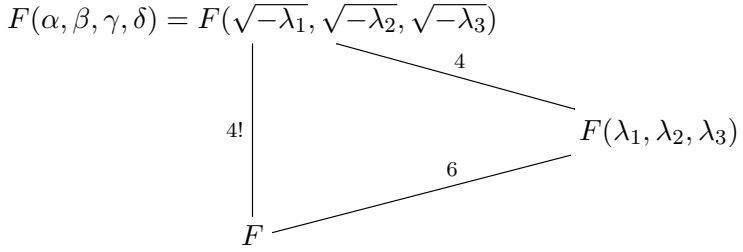
So $\sqrt{-\lambda_1}\sqrt{-\lambda_2}\sqrt{-\lambda_3} = -q$. Using this the choice of two of the three square roots determines the third choice. Evidently, the different possible choices amount to permuting the roots.

Thus it remains to solve for λ_i. The elements of S_4 permute these, therefore the coefficients of $h(x) = (x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$ belong to $\mathbb{Q}(p,q,r)$. Calculating, we get

$$h(x) = x^3 - 2px^2 + (p^2-4r)x + q^2.$$

This is the *resolvent cubic* associated to $g(x)$, which can be solved using Cardano's formula.

Note that this method proceeds by showing that if $F = \mathbb{Q}(p,q,r)$, then the splitting field $F(\alpha,\beta,\gamma,\delta)$ of $g(x)$ over F is equal to $F(\sqrt{-\lambda_1},\sqrt{-\lambda_2},\sqrt{-\lambda_3})$, which, since $\sqrt{-\lambda_1}\sqrt{-\lambda_2}\sqrt{-\lambda_3} = -q$, is the same as $F(\sqrt{-\lambda_1},\sqrt{-\lambda_2})$. There is then a diagram of fields



which depicts the reduction the quartic case to its resolvent cubic, corresponding to the extension $F(\lambda_1,\lambda_2,\lambda_3)/F$.

18. Calculating Galois groups by Reduction

Previously we saw an argument such as the following: Suppose $f(x) \in \mathbb{Q}[x]$ is an irreducible polynomial of degree p, where p is prime. Then the Galois group G of $f(x)$ is a transitive subgroup of S_p. As p divides the order of G, the latter has an element of order p, which can only be a p-cycle. Then if one can show that G has any transposition, $G = S_p$, since S_p is generated by any p-cycle and transposition. This would be the case for instance, if $f(x)$ has two complex and $p-2$ real roots, as complex conjugation would then be a transposition.

It's often the case that the Galois group of $f(x)$ is determined up to isomorphism, as a subgroup of S_n, once enough information is known about the types of cycles that appear in it.

We now present here some tools from algebraic number theory that are helpful for determining cycle type in Galois groups of polynomials over integers.

Let $K/\mathbb{Q}$ be a finite extension. An element of $a \in K$ is called an *algebraic integer* if its minimal polynomial is in $\mathbb{Z}[x]$. Let $\mathcal{O}_K \subset K$ be the set of all algebraic integers in K.

Here are some standard results from algebraic number theory, whose proofs we mostly skip.

Proposition 18.1. *$\mathcal{O}_K$ is an integral domain with fraction field K.*

To prove this, it's enough to show R is closed under addition and multiplication. It will then be an integral domain since it's a subring of a field. We omit the proof.

It's clear that any field automorphism $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$ preserves $\mathcal{O}_K$. If $I \subset \mathcal{O}_K$ is an ideal, so is $I^\sigma = \sigma(I)$.

Proposition 18.2. *(a) Any ideal $I \subset \mathcal{O}_K$ factors into a product*

$$\wp_1^{e_1} \cdots \wp_r^{e_r}$$

of distinct prime ideals $\wp_i$, and this factorization is unique up to rearrangement.

(b) If $K/\mathbb{Q}$ is Galois, and

$$(p) = \wp_1^{e_1} \cdots \wp_r^{e_r}$$

then $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the prime ideals $\wp_i$. For each $\wp_i$, we have $\wp_i \cap \mathbb{Z} = p\mathbb{Z}$.

An immediate consequence of (b) plus the uniqueness in (a) is that all the powers e_i are equal.

We say a prime ideal $\wp$ of R *lies above* p if it occurs in the factorization of (p) in R.

Example 18.3. If $K = \mathbb{Q}(i)$, then $\mathcal{O}_K = \mathbb{Z}[i]$. The ideal $5\mathcal{O}_K$ factors as

$$5\mathcal{O}_K = \wp_1\wp_2$$

where $\wp_1 = (1+2i)$, $\wp_2 = (1-2i)$. The non-trivial element of $\mathrm{Aut}(K/\mathbb{Q})$ swaps $\wp_1$ and $\wp_2$. We also have $2 = (1+i)(1-i)$ but in fact the ideals $(1+i)$ and $(1-i)$ are the same, so $2\mathcal{O}_K$ factors as

$$2\mathcal{O}_K = \wp^2$$

where $\wp = (1+i)$.

Let $\wp \subset R$ be a prime lying over $p \in \mathbb{Z}$. Then $\mathcal{O}_K/\wp$ is a *finite field* containing $\mathbb{Z}/p = \mathbb{F}_p$, so isomorphic to $\mathbb{F}_q$ for some $q = p^m$. The subgroup

$$D_\wp = \{\sigma \in G : \sigma(\wp) = \wp\}$$

is called the *decomposition* subgroup of G at $\wp$. Note that if $\sigma \in D_\wp$, it induces a field automorphism

$$\overline{\sigma} : \mathcal{O}_K/\wp \to \mathcal{O}_K/\wp, \quad \overline{\sigma}(x+\wp) = \sigma(x) + \wp.$$

Therefore there is a map

$$D_\mathfrak{p} \to \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p), \quad \sigma \mapsto \overline{\sigma}.$$

Here is one final fact we will take for granted:

Proposition 18.4. *Let $K/\mathbb{Q}$ be the splitting field of irreducible monic $f(x) \in \mathbb{Z}[x]$. Suppose p is a prime not dividing the discriminant of $f(x)$. Then $p\mathbb{Z} = \wp_1 \cdots \wp_r$ is the prime ideal factorization of $p\mathbb{Z}$ in $\mathcal{O}_K$, with $\wp_i$ distinct. For each $\wp = \wp_i$, $D_\wp \to \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is an isomorphism. In particular, $D_\wp$ is cyclic of order $[\mathbb{F}_q : \mathbb{F}_p]$, generated by the Frobenius element in $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.*

Suppose $f(x)$, p and K are as in the proposition. If $\alpha_1, \cdots, \alpha_n$ are the roots of $f(x)$, then $K = \mathbb{Q}(\alpha_1, \cdots, \alpha_n)$. The images $\overline{\alpha}_i \in \mathcal{O}_K/\wp_i$ of α_i are the roots of $\overline{f}(x) = f(x) \pmod p \in \mathbb{F}_p[x]$. As $\mathrm{Gal}(K/\mathbb{Q})$ acts on the roots of $f(x)$, $D_\wp \subset \mathrm{Gal}(K/\mathbb{Q})$ acts on the roots of $\overline{f}(x)$. However, $\overline{f}(x)$ may no longer be irreducible! This means that the generator σ of the cyclic group $D_\wp \simeq \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ acts transitively on the roots of each irreducible factor of $\overline{f}(x)$ separately. Therefore if $\overline{f}(x)$ has irreducible factors $\overline{f}_i(x)$ of degree n_i, σ is a cycle of type $(n_1, \cdots, n_l)$ in S_n. Thus by investigating the factorization of $f(x)$ modulo p, we obtain information about the possible cycle types of elements in $D_\wp \subset \mathrm{Gal}(K/\mathbb{Q})$.

Example 18.5. Let $f(x) = x^7 + x - 1$. It is irreducible, and its discriminant has prime factors, 11, 239, 331. Over $\mathbb{F}_3$, $f(x)$ factors as

$$(1 + x)(2 + 2x + x^2 + 2x^3 + x^4 + 2x^5 + x^6).$$

Then if $\wp$ is a prime of the splitting field K of $f(x)$ lying over 3, the cyclic generator of $D_\wp$ is a 6-cycle in $G = \mathrm{Gal}(K/\mathbb{Q}) \subset S_7$. Since G must also contain a 7-cycle, $G = S_7$.

This method works best when trying to prove a certain Galois group is S_n. If the Galois group is a proper subgroup of S_n, it can give heuristic information instead.

Suppose that $p \in \mathbb{Z}$ is a prime and that

$$p\mathbb{Z} = \wp_1 \wp_2 \cdots \wp_r$$

is the prime ideal factorization of $p\mathbb{Z}$ in $\mathcal{O}_K \subset K$, where K is the splitting field of monic irreducible $f(x) \in \mathbb{Z}[x]$. For each $\wp = \wp_i$, there is a decomposition group $D_{\wp_i}$, which is cyclic, generated by a distinguished element π_i that maps to the Frobenius under $D_{\wp_i} \simeq \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. For any $i, j = 1, \cdots, r$, $i \neq j$, by Proposition 18.2(b) there exists $\sigma \in \mathrm{Gal}(K/F)$ such that $\sigma(\wp_i) = \wp_j$. It follows that $\sigma^{-1} D_{\wp_j} \sigma = D_{\wp_i}$, and furthermore $\sigma^{-1}\pi_j\sigma = \pi_i$, since the image of $\sigma^{-1}\pi_j\sigma$ in $\mathrm{Aut}(k_i/\mathbb{F}_p)$, with $k_i = \mathcal{O}_K/\wp_i$ is the map

$$x \mapsto \overline{\sigma}^{-1}\overline{\pi_j\sigma}(x) = \overline{\sigma}^{-1}(\overline{\sigma}(x)^q) = x^q,$$

which is just the Frobenius $\overline{\pi}_i$.

Therefore the Frobenius elements $\pi_1, \cdots, \pi_r$ are all conjugate. In fact, for any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma^{-1}\pi_i\sigma$ is the Frobenius element of $\sigma^{-1}(\wp_i)$, so that $\{\pi_1, \cdots, \pi_r\}$ is an entire conjugacy class in G. Thus each integer prime p determines a conjugacy class F_p in $\mathrm{Gal}(K/\mathbb{Q})$ consisting of the Frobenius elements in $D_{\wp_i}$.

Theorem 18.6 (Cebotarev density theorem)**.** *Let $C \subset \mathrm{Gal}(K/\mathbb{Q})$ be a conjugacy class of size c, and $n = |\mathrm{Gal}(K/\mathbb{Q})|$. The density of primes p such that $C = F_p$ is c/n.*

The full Cebotarev density theorem is about arbitrary Galois extensions K/F as opposed to $K/\mathbb{Q}$. Note that it implies any element of G is the Frobenius of some prime $\wp$ infinitely many times.

By computing the factorization of $f(x)$ modulo p for many primes, we can compute the density of various cycles types in G. If $G \neq S_n$, it will not definitively pin down the subgroup G, but it may give a hint.

Example 18.7. The polynomial $f(x) = x^8 - x^4 + 1$ is irreducible, and its discriminant is $2^{16} \cdot 3^4$. Modulo the first 100 primes after 3, $f(x)$ fractors into a cycle of type $(2, 2, 2, 2)$ 91 times, and factors completely in the other 9 cases.

The primes modulo which $f(x)$ factors completely correspond to the conjugacy class of the identity element of G. The cycles of type $(2, 2, 2, 2)$ correspond to elements of order 2. Evidence

suggests this is the only non-trivial type, so that every non-trivial element of the Galois group has order two. In particular it's abelian, and every element is its own conjugacy class. The identity element should then occur with density $1/n \simeq 9/91$, which appears about 1 in 10. But the order of the Galois group should be divisible by 8, so we need better accuracy for our heuristics. Increasing the number of primes from 100 to 10000, we get the trivial conjugacy class 1230 times, roughly in a $1 : 8.13$ ratio.

This suggests the Galois group has order 8, and isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$, which is indeed the case.

Example 18.8. The polynomial $x^8 - x^3 + 1$ is also irreducible, with discriminant $11 \cdot 1517531$. Modulo 7 it factors as

$$(2 + x)(3 + x + 2x^2 + x^3 + 2x^4 + 4x^5 + 3x^6 + x^7)$$

so the Galois group has a 7-cycle, hence it is S_8.

19. Transcendental Extensions, Function fields

We have seen examples of infinite extensions such as $\overline{\mathbb{Q}}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$, or $F(t_1, \cdots, t_n)$, where t_i are indeterminates. Unlike finite extensions, these are not necessarily algebraic.

There's a notion of *algebraic independence* which is similar to linear independence in linear algebra.

Definition 19.1. Let E/F be a field extension. A subset $S \subset E$ is called *algebraically independent* over F, if for any $s_1, \cdots, s_n \in S$, and any non-zero polynomial $f(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$, $f(s_1, \cdots, s_n) \neq 0$.

In other words, $s_1, \cdots, s_n$ are algebraically independent if they satisfy no algebraic relations among themselves. Clearly if $S \subset E$ is algebraically independent over F, it can not contain any elements that are algebraic over F. In particular, if E/F is finite, E has no non-empty subsets that are algebraically independent over F.

If $S_1 \subset S_2 \subset S_3 \subset \cdots$ are subsets of E that are algebraically independent over F, so is $S = \cup_i S_i$. That implies that Zorn's lemma applies to algebraically independent subsets of E, and guarantees the existence of the following.

Definition 19.2. A *transcendental base* of E over F is an algebraically independent set S that is maximal with respect to inclusion.

Here is a theorem we state without proof.

Theorem 19.3. *Any two transcendence bases for E/F have the same cardinality.*

Note the similarity to the theorem that says any two bases for a vector space have the same cardinality. In fact the proof is similar.

The cardinality of a transcendence base S is called the *transcendence degree* of E/F. Let E/F be a field extension and $S \subset E$ a transcendental base for E over F. Then $F(S)$ is a *purely transcendental* extension of F: it is generated by an algebraically independent set.

Proposition 19.4. *Let $S \subset E$ be a transcendental base over F. Then $E/F(S)$ is algebraic.*

Proof. Let $x \in E$. If x is not algebraic over $F(S)$, then $S' = S \cup \{x\}$ is algebraically independent over F and strictly contains S, which contradicts the maximality of S. □

Therefore an *arbitrary* extension E/F can be decomposed into extensions $E/F(S)$ and $F(S)/F$, where $E/F(S)$ is algebraic and $F(S)/F$ purely transcendental.

Example 19.5. The extension $\mathbb{Q}(t_1, t_2)/\mathbb{Q}$ is purely transcendental, generated by the transcendental base $\{t_1, t_2\}$. Likewise $\mathbb{Q}(\pi)/\mathbb{Q}$ and $\mathbb{Q}(e)/\mathbb{Q}$ are purely transcendental. It is conjectured, but not known, that $\mathbb{Q}(e, \pi)$ is purely transcendental over $\mathbb{Q}$. In other words, it's an open problem to prove that e and π are algebraically independent over $\mathbb{Q}$.

Example 19.6. Let C be an *algebraic curve*, given by

$$\{(a,b) \in \mathbb{C}^2 : f(a,b) = 0\}$$

where $f(x,y) \in \mathbb{C}[x,y]$ is an irreducible polynomial, e.g.

$$f(x,y) = y^2 - x^3 - x.$$

The elements of $\mathbb{C}[x,y]$ give polynomial functions on the curve C. For instance $p(x,y) = y^2 - x^3$ defines a function

$$C \to \mathbb{C}, \quad (a,b) \mapsto a^3 + b^2.$$

But note that for $(a,b) \in C$ we have $b^2 - a^3 = -a$, so the polynomial $q(x,y) = -x$ defines the same function $C \to \mathbb{C}$. The set of all polynomial functions on C is therefore not $\mathbb{C}[x,y]$ but its quotient

$$A = \mathbb{C}[x,y]/(y^2 - x^3 - x).$$

Now $(y^2 - x^3 - x)$ is a prime ideal of $\mathbb{C}[x,y]$, so A is an integral domain. Its fraction field K corresponds to rational functions on C, e.g

$$h(x,y) = \frac{x^2+1}{y^2 - x}.$$

The rational functions are only defined on some open subset of C. For instance if $(a,b) = (0,0)$, then $(a,b) \in C$ but $h(a,b)$ is not well-defined, since the denominator is zero.

Now consider $\mathbb{C}(x) \subset K$. The element $x \in K$ satisfies not algebraic relation with coefficients in $\mathbb{C}$. However $y \in K$ is the root of $g(t) = t^2 - x^3 - x \in \mathbb{C}(x)$, and we know x, y generate K over $\mathbb{C}$. Therefore K is a field of transcendence degree 1 over $\mathbb{C}$, but *not* purely transcendental.

It's a well-known theorem in algebraic geometry that a field extension $K/\mathbb{C}$ has transcendence degree 1 if and only if it's the field of rational functions of some algebraic curve. In other words, any such K is the *function field* of some curve. For instance, the purely transcendental field $\mathbb{C}(x)$ is the function field of the *affine line* $\mathbb{A}^1$, which is the complex plane considered as a complex curve.

Suppose C_1, C_2 are algebraic curves with function fields K_1, K_2. Let $f : C_1 \to C_2$ be a rational function, which may only be defined on some open subset of C_1. To each $g \in K_2$, corresponding to a rational function $g : C_2 \to \mathbb{C}$, we can then associate $g \circ f : K_1 \to \mathbb{C}$. Thus we get a field homomorphism

$$K_2 \to K_1, \quad g \mapsto g \circ f,$$

which is necessarily *injective*. In other words, a rational map $f : C_1 \to C_2$ corresponds to an inclusion of fields $K_2 \subset K_1$. Note that since K_1, K_2 both have transcendence degree 1 over $\mathbb{C}$, the extension K_1/K_2 must be algebraic!

Thus there is a dictionary between algebraic extensions of function fields of transcendence degree 1, and algebraic curves with rational maps between them. Such relations are the basis of algebraic geometry.

Example 19.7. Let C be the curve defined by the equation $y^2 = x^3 + x$ as before, and K its function field. Then $x \in K$ is a rational function on C:

$$C \to \mathbb{A}^1, \quad (a,b) \mapsto a$$

corresponding to the algebraic extension of fields

$$\mathbb{C}(x) \hookrightarrow K = \mathbb{C}(x)[y]/(y^2 - x^3 - x).$$

Note that K is a degree 2 extension of $\mathbb{C}(x)$. This can be seen geometrically, as the map $C \to \mathbb{A}^1$, $(a,b) \mapsto a$ is two-to-one: it maps (a,b) and $(a,-b)$ to the same point. Algebraicallly, $K/\mathbb{C}(x)$ is Galois, with Galois group of order 2. The non-trivial element corresponds to the field automorphism that fixes $\mathbb{C}(x)$ and sends y to $-y$. It corresponds to the rational function

$$C \to C, \quad (a,b) \mapsto (a,-b)$$

which captures the symmetry of $C \to \mathbb{A}^1$.

Consider now the map

$$C \to \mathbb{A}^1, \quad (a, b) \mapsto b.$$

It corresponds to the field embedding $\mathbb{C}(y) \hookrightarrow K$, where now we may consider

$$K = \mathbb{C}(y)[x]/(x^3 + x - y^2).$$

Here we now we have taken y to be the transcendental base of K, and considered x as a root of $p(t) = t^3 + t - y^2$, adjoined to $\mathbb{C}(y)$. Let L be the splitting field of $p(t)$ over K, generated by the three roots α, β, γ of $t^3 + t - y^2$. These roots must satisfy

$$\alpha + \beta + \gamma = 0, \quad \alpha\beta + \beta\gamma + \alpha\gamma = 1, \quad \alpha\beta\gamma = y^2.$$

If we take $\alpha = x$, we obtain the equations

$$\beta + \gamma = -x, \quad \beta\gamma = \frac{y^2}{x} = x^2 + 1$$

so that β, γ are the roots of $u^2 + ux + x^2 + 1$, i.e.

$$\frac{-x \pm \sqrt{-3x^2 - 4}}{2}.$$

It follows that $L = K(\alpha)$, where $\alpha^2 = -3x^2 - 4$, and $L/\mathbb{C}(y)$ has degree 6, with Galois group S_3.

Thus there are two subfields K_1, K_2 of L, which have degree 3 over $\mathbb{C}(y)$, and are isomorphic to K. They will correspond to curves C_1 and C_2 which are *birationally* isomorphic to C. The field L will correspond to a curve D, admitting two-to-one coverings onto all three curves C, C_1, and C_2.

20. Representation Theory

In the contexts in which they arise, groups often *act* on another object. We have already seen this with permutations. If a group G permutes a set S of n elements, we have a map $\pi : G \to S_n$. An analogue of this situation is when a group acts on a *vector space*.

Definition 20.1. A *representation* of a group G is a pair (π, V), where V is a vector space over some field F, and $\pi : G \to \mathrm{GL}(V)$ is a group homomorphism.

Sometimes π or V is used to denote the pair (π, V), the other member of the pair being implied.

We will be mainly concerned with representations of *finite* groups G on *finite-dimensional* vector spaces V. If an isomorphism $V \simeq F^n$ is fixed, the representation π can be written as a group homomorphism $G \to \mathrm{GL}_n(F)$.

A representation is called *faithful* if it's injective. In that case the group itself is identified as a subgroup of a matrix group. This is similar to embedding a group in S_n.

Another way to talk about representations is to identify them with *modules* over a certain ring, which we now define.

Definition 20.2. Let F be a field and $G = \{g_1, \cdots, g_n\}$ a finite group. The *group-ring* FG is the ring whose elements are formal sums

$$x = \sum_{i=1}^{n} a_i g_i, \quad a_g i \in F.$$

Then if $y = \sum_{j=1}^{n} b_i g_i$, the ring operations are defined by

$$x + y = \sum_{i=1}^{n} (a_i + b_i) g_i, \quad x \cdot y = \sum_{k=1}^{n} \sum_{\substack{i,\, j \\ g_i g_j = g_k}} a_i b_j g_k.$$

It's convenient to arrange that g_1 be the identity element of G. Then the multiplicative identity of the ring FG is $1g_1$.

The map $F \to FG$, $a \mapsto a \cdot g_1$ is an embedding of F into the center of FG. This makes FG into an *F-algebra*.

Suppose V is an FG-module. Since $F \subset FG$ it is in particular an F-vector space. Then $g \in G$ acts on V by left-multiplication by $1g$. This gives a map $\pi : G \to \mathrm{GL}(V)$ so that (π, V) is a representation. Conversely, suppose $\pi : G \to V$ is given. Then an element $x = \sum_{i=1}^n a_i g_i$ can be made to act on V by

$$x \cdot v = \sum_{i=1}^n a_i \pi(g_i) v.$$

Therefore an FG-module and a representation of G are *equivalent*. Which terminology is used in practice depends on the context. Since we have already learned about modules, it is convenient to describe the various features of representation theory in those terms.

Example 20.3. Let $V = FG$ considered as an FG-module. The action of G is given by

$$g \cdot \sum_{i=1}^n a_i g_i = \sum_{i=1}^n a_i g g_i.$$

This is called the *(left-)regular* representation of G over F.

Example 20.4. Let $\mathbb{H} = \{x = a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ be Hamilton's quaternions. Consider the map

$$\varphi : H \to \mathrm{GL}_2(\mathbb{C}), \quad \varphi(x) = \begin{pmatrix} a + bi & -c - di \\ c - di & a - bi \end{pmatrix}.$$

This is in fact a homomorphism of $\mathbb{R}$-algebras. Its image is all matrices of the form $\begin{pmatrix} z & -w \\ \overline{w} & \overline{z} \end{pmatrix}$. Let $V \subset \mathrm{GL}_2(\mathbb{C})$ denote the subset of such matrices with trace zero. Let H^1 denote the quaternions of norm 1: those with $x\overline{x} = a^2 + b^2 + c^2 + d^2 = 1$. Then

$$\pi : H \to \mathrm{GL}(V), \qquad \pi(x)(m) = \varphi(x) m \varphi(x)^{-1}$$

is a representation of H on $\mathrm{GL}(V)$.

Example 20.5. Let K/F be a finite Galois extension, and $G = \mathrm{Gal}(K/F)$. Then $\sigma \in G$ acts on K as an F-vector space. This corresponds to the representation $G \hookrightarrow \mathrm{GL}_F(K)$.

Definition 20.6. An *invariant subspace* of a representation (π, V) is a vector subspace $U \subset V$ such that $\pi(g)u \in U$ for all $u \in U$, $g \in G$.

If U is an invariant subspace of V, the map $\pi : G \to \mathrm{GL}(U)$ is well-defined., and (π, U) is a *subrepresentation* of (π, V). In the language of FG-modules a subrepresentation is exactly a submodule.

Example 20.7. The invariant subspaces of the (left) regular representation correspond to the *left ideals* of FG. For instance, consider the F-linear map $\epsilon : FG \to F$ given by

$$\epsilon(\sum_{i=1}^n a_i g_i) = \sum_{i=1}^n a_i.$$

It is a ring homomorphism called the *augmentation map*. Its kernel I is the *augmentation ideal*. As such it corresponds to a G-invariant subspace of FG of dimension $n - 1$.

Suppose that (π, V) and (ρ, W) are representations of G. An *intertwining map* $T : V \to W$ is a linear operator such that

$$T(\pi(g)v) = \rho(g)T(v), \quad \forall g \in G,\ v \in V.$$

An intertwining map corresponds to a homomorphism of FG-modules.

Definition 20.8. Two representations (π, V), (ρ, W) are equivalent if there is an invertible intertwining operator $T : V \to W$.

Equivalence of representations corresponds to isomorphism of FG-modules.

Example 20.9. Let G be any finite group, and $V = \{f : G \to \mathbb{C}\}$, the set of all complex valued-functions. Then we define an $\mathbb{C}G$-module structure on V by $(g \cdot f)(x) = f(g^{-1}x)$.

We check for instance that

$$(gh) \cdot f = g \cdot (h \cdot f).$$

Writing f_h for $h \cdot f$ we have

$$(g \cdot (h \cdot f))(x) = (g \cdot f_h)(x) = f_h(g^{-1}x) = f(h^{-1}g^{-1}x) = f((gh)^{-1}x) = (gh \cdot f)(x).$$

Note that $\mathbb{C}G$ is in fact isomorphic to V as a complex vector space. Explicitly, $T : \mathbb{C}G \to V$ sends $1 \cdot g$ to the function $\delta_g : G \to \mathbb{C}$, where $\delta_g(h) = 1$ if $h = g$ and zero otherwise. Note that

$$g \cdot \delta_h(x) = \delta_h(g^{-1}x) = 1 \iff g^{-1}x = h \iff x = gh.$$

This shows $g \cdot T(h) = g \cdot \delta_h = \delta_{gh} = T(gh)$. Then $T : \mathbb{C}G \to V$ is an intertwining map that shows V is equivalent to the regular representation of G

21. Representations of Finite Groups, Maschke's Theorem

Definition 21.1. A representation (π, V) of G is *irreducible* if it has no G-invariant subspace aside from V itself and 0, otherwise it is called reducible. It is called *completely reducible* if it is a direct sum of irreducible representations, called its *constituents*.

An irreducible representation of G is the same thing as a simple FG-module. Note that an irreducible representation is completely reducible, since it's the direct sum of itself and the zero representation. Though it might sound like conflicting terminology, this is actually okay, because completely reducibility means reducibility *to irreducibles*, i.e. the constituents.

Given two representations (π_1, V_1), (π_2, V_2) of G, we can take their direct sum $(\pi, V) = (\pi_1, V_1) \oplus (\pi_2, V_2)$. More precisely, $V = V_1 \oplus V_2$, and

$$\pi(g)(v_1 + v_2) = \pi_1(g)v_1 + \pi_2(g)v_2.$$

Then V_1, V_2 are G-invariant subspaces of V.

It's clear that if a representation is irreducible, it can not be the direct sum of two non-zero representations. The converse however is *not* true in general.

Definition 21.2. A representation (π, V) is *indecomposable* if it can not be written as a direct sum of two representations $V_1 \oplus V_2$.

The definition in terms of modules is the same: a module M over a ring R is indecomposable if it can not be written as $M_1 \oplus M_2$, with non-zero R-modules M_i. An irreducible representation of G over F is "the same thing" as an FG-module.

Example 21.3. Let $G = \mathbb{Z}$ act on $\mathbb{C}^2$ via $\pi : \mathbb{Z} \to \mathrm{GL}_2(\mathbb{C})$, where

$$\pi(n) = \begin{pmatrix} 1 & n \\ & 1 \end{pmatrix}.$$

Then π is indecomposable but not irreducible.

Indeed, if $\{e_1, e_2\}$ is the standard basis for $\mathbb{C}^2$, then $\mathbb{C}e_2$ is a G-invariant subspace of $\mathbb{C}^2$. This shows π is not irreducible. However, if $(\pi, \mathbb{C}^2) = (\pi_1, V_1) + (\pi_2, V_2)$ then V_1, V_2 must be lines, if non-zero. That would imply the action of the elements of G are simultaneously diagonalizable. But we know that $\pi(1)$ is not diagonalizable.

This example shows that in general an arbitrary representation may not be *completely reducible*, i.e. a direct of irreducibles.

However, for representations of finite groups over fields of characteristic zero, this is always the case. More precisely:

Theorem 21.4 (Maschke)**.** *Let G be a finite group over a field F such that* $\mathrm{char}(F) \nmid |G|$. *If (π, V) is a representation of G, and $U \subset V$ is a G-invariant subspace, then $V = U \oplus W$ for another G-invariant subspace $W \subset V$.*

Note that the condition on characteristic is always satisfied if $\mathrm{char}(F) = 0$.

Recall that a *projection* operator on an R-module M is an R-linear homomorphism $T : M \to M$ such that $T^2 = T$. Given a projection operator T, one obtains a decomposition of M into direct sums:

$$M = \mathrm{im}(T) \oplus \ker(T), \quad x \mapsto (T(x), x - T(x)).$$

Conversely, if $M = M_1 \oplus M_2$ is a direct sum decomposition, then the map $T(x_1, x_2) = (x_1, 0)$ is a projection operator with $\mathrm{im}(T) = M_1$, $\ker(T) = M_2$. Therefore if M' is an R-submodule of M, writing $M = M' \oplus M''$ for some complementary submodule M'' is equivalent to finding a projection operator T whose image is M_1.

Let V be a vector space over F, and $U \subset V$ a subspace. Then there always exists a subspace W such that $V = U \oplus W$, so there always exists a projection $T \in \mathrm{End}_F(V)$ with $\mathrm{im}(T) = U$.

Now assume V is a representation of G, and $U \subset V$ is a G-invariant subspace. If we consider U and V as FG-modules, the map $T : V \to V$ satisfies $T^2 = T$ and is F-linear. However, ther it may not be FG-linear, so it won't lead to a decomposition of $V = U \oplus W$ of FG-modules.

The idea of the proof of Maschke's theorem is that this failure of $T : V \to V$ to be FG-linear can sometimes be fixed by an *averaging* procedure.

Suppose $T : V \to V$ is an F-linear projection operator. If T is not FG-linear, there exists some $g \in G$ and $v \in V$ such that $T(gv) \neq gT(v)$. Substituting $v = g^{-1}v_0$ this can be written as $T(v_0) \neq gT(g^{-1}v_0)$ for some v_0, or just $T \neq gTg^{-1}$.

Lemma 21.5. *(π, V) be a representation of a group G over F, $U \subset V$ an invariant subspace.*

1. *If T is an F-linear projection with $\mathrm{im}(T) = U$, then so is $T' = gTg^{-1}$.*
2. *If $T_1, \cdots, T_n$ are F-linear projections with $\mathrm{im}(T_i) = V$, and $n \nmid \mathrm{char}(F)$, then so is*

$$T = \frac{1}{n} \sum_{i=1}^{n} T_i.$$

Proof. (1): We have

$$T' \circ T' = gTg^{-1} \circ gTg^{-1} = gT^2g^{-1} = gTg^{-1} = T'.$$

so T' is a projection operator.

Since U is G-invariant, for each $v \in V$ we have

$$\mathrm{im}(Tg^{-1}) \subset \mathrm{im}(T) \Longrightarrow \mathrm{im}(gTg^{-1}) \subset g\,\mathrm{im}(T) \subset gU \subset U.$$

Conversely, if $u \in U$, then $gTg^{-1}(u) = gT(g^{-1}u) = g(g^{-1}u) = u$, and so $U \subset \mathrm{im}(gTg^{-1})$. Therefore the image of the operator gTg^{-1} is U.

(2): Note it's enough to show $\mathrm{im}(T) \subset U$, and that $T(u) = u$ for $u \in U$. Now the first follows from the fact that $\mathrm{im}(T_i) \subset U$. For the second, we have

$$T(u) = \frac{1}{n} \sum_{i=1}^{n} T_i(u) = \frac{1}{n} \sum_{i=1}^{n} u = u.$$

□

Proof of Maschke's theorem. Suppose (π, V) is a representation of G, and $U \subset V$ a G-invariant subspace. Let $T : V \to U$ be an F-linear projection onto U. Then by the lemma

$$S = \frac{1}{|G|} \sum_{g \in G} gTg^{-1}$$

is also an F-linear projection operator onto U. In fact, S is FG-linear: for each $h \in G$ we have

$$hSh^{-1} = \frac{1}{|G|} \sum_{g \in G} hgTg^{-1}h^{-1} = \frac{1}{|G|} \sum_{g \in G} gTg^{-1} = S.$$

□

Corollary 21.6. *If F is a field, and G is a finite group, whose order does not divide the characteristic of F, then every finite dimensional representation of G over F is completely reducible.*

Proof. Let V be such a representation. Let V_1 be a *minimal* non-zero invariant subspace of V, which exists because V has finite dimension. Then V_1 is irreducible. If $V_1 = V$, then nothing is to be done. If $V_1 \subsetneq V$, then by the theorem $V = V_1 \oplus V_1'$, for another invariant subspace V_1'. If V_1' is irreducible, we are done. If not $V_1' = V_2 \oplus V_2'$ for an irreducible subrepresentation $V_2 \subset V_1'$, and we have $V = V_1 \oplus V_2 \oplus V_2'$. Continuing on inductively, some $V_n' = V_n$ has to be irreducible because $\dim V_1 > \dim V_2 > \dim V_3 > \cdots$, therefore $V = V_1 \oplus \cdots \oplus V_n$, with each factor being irreducible. □

22. Wedderburn's theorem I

Lemma 22.1. *Let G be a finite group. A representation (π, V) of G over a field F is finite-dimensional if and only if V is a finitely generated FG-module.*

Proof. A basis of V generates V as an FG-module, so if it is finite-dimensional it's also finitely generated. Conversely, suppose $\{v_1, \cdots, v_n\}$ is a finite set of generators of V as an FG-module. Then $\{\pi(g)v_i : g \in G,\ 1 \leq i \leq n\}$ is a finite set since G is finite, and spans V as an F-vector space. It therefore contains a basis, so V is finite dimensional. □

Definition 22.2. A module M over a ring R is called *semisimple* if it is a direct sum of simple R-modules.

If (π, V) is a representation of G, then it is completely reducible if and only V is semisimple as an FG-module.

Let G be a finite group, F a field with $\mathrm{char}(F) \nmid |G|$. Corollary 21.6 to Maschke's theorem then says FG is a semisimple ring. Then every (finite dimensional) representation of G over F is a direct sum of irreducible ones. Thus to have a complete picture of all the representations of G (over F, of finite dimension) it's enough to classify all the irreducible ones. It turns out there's a convenient way to do this via the regular representation.

Recall that the regular representation of G is the ring FG as a left-module over itself. Since it is semisimple, it decomposes into a direct sum

$$FG = J_1 \oplus \cdots \oplus J_m,$$

where J_i are simple FG-submodules of FG, i.e ideals. If we group the isomorphic ideals together, we can write

$$FG \simeq I_1^{n_1} \oplus \cdots \oplus I_r^{n_r}$$

with $I_i \not\simeq I_j$ if $i \neq j$. Wedderburn's theorem describes the action of G on each I_i piece.

We only aim to state Wedderburn's theorem, but for even the statement to make sense we need a few facts from representation theory. The following lemma is a fundamental one:

Lemma 22.3 (Schur)**.** *Suppose that M, M' are simple R-modules, and $D = \mathrm{Hom}_R(M, M')$. If $M \simeq M'$, then D is a division ring, otherwise it is zero.*

Proof. Homework. □

Corollary 22.4. *Let $M \cong M_1^{n_1} \oplus \cdots \oplus M_r^{n_r}$ be a semisimple R-module, with simple constituents M_i that are distinct up to isomorphism. If $D_i = \mathrm{End}_R(M_i)$, then we have an isomorphism of R-algebras*

$$\mathrm{End}_R(M) \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r).$$

Proof. For each simple factor M_i, we have $\mathrm{End}_R(M_i^{n_i}) \cong M_{n_i}(\mathrm{End}_R(M_i)) = M_{n_i}(D_i)$. Since $\mathrm{Hom}_R(M_i, M_j) = 0$ for $i \neq j$, we have

$$\mathrm{End}_R(M) \cong \bigoplus_{1 \leq i,j \leq r} \mathrm{Hom}_R(M_i^{n_i}, M_j^{n_j}) \cong \bigoplus_{i=1}^{r} \mathrm{End}_R(M_i^{n_i}) \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r).$$

It's not hard to see that this isomorphism is compatible with the ring structures, meaning composition of endomorphisms on the left corresponds to matrix multiplication in each factor on the right hand side. □

Let us apply the corollary to the decomposition

$$FG = I_1^{n_1} \oplus \cdots I_r^{n_r}.$$

For $S = \mathrm{End}_{FG}(FG)$ we have

$$S = M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r),$$

where D_i are division rings. The natural inclusion $F \hookrightarrow FG \subset S$ on the left-hand side induces inclusions $F \hookrightarrow D_i$ on the right. In other words, D_i are division *algebras* over F.

On the other hand, the ring S is canonically isomorphic to the *opposite* ring R^{op}. If $R = (R, +, \cdot)$, $R^{\mathrm{op}} = (R, +, *)$, where $x * y = y \cdot x$.

Lemma 22.5. *Let R be a ring. The maps*

$$\mathrm{End}_R(R) \longrightarrow R, \quad f \mapsto f(1),$$

and

$$R \longrightarrow \mathrm{End}_R(R), \quad r \mapsto f_r, \quad f_r(x) = x \cdot r$$

give ring isomorphisms $R^{\mathrm{op}} \cong \mathrm{End}_R(R)$.

Proof. We have $f_r(1) = r$. If $f : R \to R$ is R-linear,

$$f(x) = f(x \cdot 1) = xf(1).$$

This shows the given maps are mutual inverses, and so bijective. It's clear they are additive. We find

$$f_{rs}(x) = xrs = f_s(xr) = f_s \circ f_r(x),$$

which shows the $f \mapsto f(1)$ maps composition in $\mathrm{End}_R(R)$ to the multiplication operation in R^{op}. □

Applying this lemma to $R = FG$, we get $S = \mathrm{End}_{FG}(FG) \cong FG^{\mathrm{op}}$, or what's the same $S^{\mathrm{op}} \cong FG$. Since the opposite of a division ring is again a division ring, we obtain two decompositions

$$FG = M_{n_1}(D_1) \oplus \cdots M_{n_1}(D_r),$$

as a ring and

$$FG = I_1^{n_r} \oplus \cdots \oplus I_r^{n_r}$$

as an FG-module, where $D_i^{\mathrm{op}} = \mathrm{End}_{FG}(I_i)$.

The action of FG on each I_i piece is through the quotient map $FG \twoheadrightarrow M_{n_i}(D_i)$. Then since I_i are simple FG-modules, each I_i is also a simple $M_{n_i}(D_i)$-module. Wedderburn's theorem says that in fact, up to isomorphism, there is only one simple $M_{n_i}(D_i)$ module, and that is the column vectors $D_i^{n_i}$ on which $M_{n_i}(D_i)$ acts by matrix multiplication on the left.

It turns out that if M is *any* simple FG-module, it will have to be a simple module over one of the factors $M_{n_i}(D_i)$ of FG, and therefore isomorphic to one of the I_i. That means every irreducible

representation of G occurs as a factor in the left-regular representation. We will only need need this statement over $\mathbb{C}$:

Theorem 22.6 (Wedderburn's Theorem over $\mathbb{C}$)**.** *Let G be a finite group. There is a decomposition of $\mathbb{C}$-algebras*

$$\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_r}(\mathbb{C}),$$

where $M_{n_i}(\mathbb{C})$ is the $\mathbb{C}$-algebra of $n_i \times n_i$ matrices. Furthermore, there exist exactly r inequivalent irreducible complex representations $V_1, \cdots, V_r$ of G, of dimensions $n_1, \cdots, n_r$. Each V_i is isomorphic as a $\mathbb{C}G$-module to $\mathbb{C}^{n_i}$ on which G acts through the quotient $\mathbb{C}G \to M_{n_i}(\mathbb{C})$ by matrix multiplication.

In particular, one has

$$|G| = \dim_{\mathbb{C}} \mathbb{C}G = n_1^2 + \cdots n_r^2,$$

where n_i are the degrees of the distinct irreducible representations of G (up to equivalence). Let us demonstrate this theorem with an example.

Example 22.7. Let $G = S_3$, $F = \mathbb{C}$. Let $V = \{f : S_3 \to \mathbb{C}\}$ be the vector space of all $\mathbb{C}$-valued functions on G, and let G act on V by

$$\pi : G \to \mathrm{End}(V), \quad (\pi(g)f)(x) = f(g^{-1}x).$$

We saw in Example 20.9 that (π, V) is equivalent to the regular representation $\mathbb{C}G$.

Let $V_0 = V_1 = \mathbb{C}$. Define $\chi_0 : S_3 \to \mathrm{GL}(V_0) = \mathbb{C}^\times$ to be the trivial character $\chi_0 \equiv 1$, and $\chi_1 : S_3 \to \mathrm{GL}(V_1)$ to be the sign character $\chi_1(g) = \mathrm{sgn}(g)$.

Let V_2 be the subspace of $\mathbb{C}^3$ orthogonal to the vector $(1, 1, 1)$, i.e.

$$V_2 = \{(z_1, z_2, z_3) \in \mathbb{C}^3 : z_1 + z_2 + z_3 = 0\}.$$

Let $\pi_2 : S_3 \to \mathrm{GL}(V_2)$ be the representation

$$\pi_2(\sigma)(z_1, z_2, z_3) = (z_{\sigma(1)}, z_{\sigma(2)}, z_{\sigma(3)}).$$

This is called the *standard representation* of S_3. There is a similarly defined standard representation for each S_n, and they are all irreducible.

Now note V_0, V_1, V_2 have dimensions $1, 1, 2$, and $1^2 + 1^2 + 2^2 = 6 = \dim_{\mathbb{C}} \mathbb{C}G$. Wedderburn's theorem then implies that

$$\mathbb{C}G \cong \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C}),$$

and that (χ_0, V_0), (χ_1, V_1), and (π_2, V_2) are up to equivalence all the irreducible representations of S_3. By Maschke's theorem any finite dimensional complex representation of S_3 must be equivalent to $V_0^{n_0} \oplus V_1^{n_1} \oplus V_2^{n_2}$ for some integers $n_i \geq 0$.

Note that in Wedderburn's theorem an irreducible representation of dimension n corresponds to a factor of dimension n^2 in $\mathbb{C}G$.

23. Wedderburn's Theorem II

Definition 23.1. Let R be a ring.

(1) An element $e \in R$ is called an *idempotent* if $e^2 = e$.
(2) Two idempotents e_1, e_2 are called *orthogonal* if $e_1 e_2 = e_2 e_1 = 0$.
(3) A *primitive* idempotent is one that can not be written as a sum of non-zero orthogonal idempotents.
(4) An idempotent $e \in R$ is *central* if $e \in Z(R)$.
(5) An idempotent $e \in R$ is *central primitive* if it's central, and primitive in $Z(R)$.

Example 23.2. Let (π, V) be a completely reducible representation of a group G over a field F, and $V = V_1 \oplus \cdots \oplus V_r$ a decomposition into constituents (π_i, V_i). Let $T_i : V \to V$ be the FG-linear projection operators with $\mathrm{im}(T_i) = V_i$. Note that

$$T_i^2 = T_i, \quad T_i T_j = T_j T_i = 0 \text{ for } i \neq j, \quad T_1 + T_2 + \cdots + T_r = \mathrm{Id}.$$

The FG-module V is a module over $S = \mathrm{End}_{FG}(V)$. The projections T_i are orthogonal, central primitive idempotents in S. These are easy to check consequences of the definitions, with primitivity following from the irreducibility of the V_i.

Proposition 23.3. *Let D be a division algebra, $R = M_n(D)$.*

(a) *R has no two-sided ideals aside from R itself and 0.*
(b) *The center of R consists of scalar matrices aI, where $a \in Z(D)$.*
(c) *If e_i is the diagonal matrix with a 1 at the (i,i)th entry and zero elsewhere, then $e_1, \cdots, e_n$ are primitive orthogonal idempotents.*
(d) *For each i, Re_i is a simple R-module, isomorphic to the column vectors D^n as an R-module.*
(e) *Up to isomorphism $I = D^n$ is the unique non-zero simple R-module. In particular, $R \cong I^n$ as an R-module.*

Proof. For $1 \leq i, j \leq n$, let $E_{ij} \in M_n(D)$ denote the matrix with a 1 at the (i,j)th entry, and zeros elsewhere. Note that for $1 \leq i, j, k \leq n$,

$$E_{ij} E_{j'k} = E_{ik} \text{ if } j = j', \ 0 \text{ otherwise.}$$

Let J be a non-zero two-sided ideal of R. We claim that if $E_{ij} \in J$, then $J = R$. Indeed, in that case we have

$$E_{pq} = E_{pi} E_{ij} E_{jq}$$

so $E_{pq} \in J$, for any $1 \leq p, q \leq n$. Then,

$$1 = \sum_{p,q} E_{pq} \in J \Longrightarrow J = R.$$

Now $J \neq 0$, so J contains a matrix $A = (a_{pq})$ with some $a_{ij} \neq 0$. Then

$$E_{ii} A E_{jj} = a_{ij} E_{ij} \in J.$$

Then since D is a division algebra, $E_{ij} \in J$, so $J = M_n(D)$. This proves (a).

Let $A = (a_{ij}) \in R$ be in the center. Then for $j \neq i$, we have

$$a_{ij} E_{ij} = E_{ii} A E_{jj} = A E_{ii} E_{jj} = 0 \Longrightarrow a_{ij} = 0,$$

so A must be a diagonal matrix. Then

$$a_{ii} E_{11} = E_{1i} A E_{i1} = A E_{1i} E_{i1} = A E_{11} = A E_{11}^2 = E_{11} A E_{11} = a_{11} E_{11},$$

so in fact $A = aI$, for some $a \in D$, and I the $n \times n$ identity matrix. For any $b \in D$, we have

$$(ab)I = (aI)b = Ab = bA = b(aI) = (ba)I \Longrightarrow ab = ba \ \forall b \in D \Longrightarrow a \in Z(D).$$

Conversely any $a \in Z(D)$ lies in the center of R, so this shows (b).

It's clear that $e_i = E_{ii}$ are orthogonal idempotents, and that Re_i is a left R-module. Any $A \in Re_i$ consists of matrices with only the ith column nonzero. Let $A = (a_{pq}) \in Re_i$ be any non-zero element, so that $a_{pi} \neq 0$ for some p. Then

$$a_{pi}^{-1} E_{ip} A = a_{pi}^{-1} (a_{pi} E_i i) = e_i.$$

Then any non-zero submodule of Re_i contains e_i, and hence is equal to Re_i. This shows that Re_i is simple.

Now if any $e_i = e_i' + e_i''$ for orthogonal idempotents e_i' and e_i'', then $Re_i = Re_i' \oplus Re_i''$, which shows either e_i' or $e_i'' = 0$, since Re_i is simple. This shows (c).

Since

$$D^n \to Re_i, \quad (d_1, \cdots, d_n) \mapsto d_1 E_{1i} + \cdots d_n E_{ni}$$

is an isomorphism of R-modules, each Re_i is isomorphic to D^n. This shows (d).

Suppose M is any non-zero simple R-module. If $m \in M$ is non-zero, we have $m = e_1 m + e_2 m + \cdots e_n m$, so some $e_i m \neq 0$. then

$$Re_i \to M, \quad re_i \mapsto re_i m$$

is a non-zero map. Since Re_i is also simple, it must be an isomorphism.

Now for $I = D^n$, we have

$$R = Re_1 \oplus \cdots \oplus Re_n \simeq I^n.$$

This shows (e). □

Definition 23.4. A ring R is said to be *left-Artinian*, if it satisfies the *descending condition on ideal chains* (DCC): any chain of left ideals

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$$

eventually stabilizes, meaning there exists n_0 such that $I_n = I_{n_0}$ for $n \geq n_0$. A ring R is called *semisimple* if it's left-Artinian and any left R-module is semisimple.

Example 23.5. Let G be a finite group, and F a field with $\mathrm{char}(F) \nmid |G|$. By Maschke's theorem the ring FG is semisimple. It also satisfies DCC: If $I_1 \supset I_2 \supset \cdots$ is a descending chain of ideals in FG, then each I_n is an F-vector space of finite dimension, hence the chain can not strictly decrease in dimension forever.

Definition 23.6. An R-module Q is called *injective*, if whenever $f : Q \hookrightarrow M$ is an injective morphism of R-modules, and $Q' = f(Q)$, there exists a submodule $N \subset M$ such that $M = Q' \oplus N$.

Example 23.7. Both $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are injective $\mathbb{Z}$-modules. This is left as exercise to prove. If R is a field, any R-module, i.e. a vector space over R, is injective.

Example 23.8. Let G be finite, and F a field with $\mathrm{char}(F) \nmid |G|$. Then Maschke's theorem says every FG-module is injective.

There is also a notion dual to an injective module.

Definition 23.9. An R-module P is called *projective* if whenever $\phi : M \twoheadrightarrow P$ is a surjective R-linear map, there exists an R-submodule $N \subset M$ and an isomorphism $M \simeq N \oplus P$ that identifies ϕ with the projection onto P.

Here's the full statement of Wedderburn's theorem, whose proof we skip. They can be found as exercises in Dummit and Foote.

Theorem 23.10 (Wedderburn)**.** *Let R be a ring. The following are equivalent:*

(a) *R is semisimple as a module over itself.*
(b) *Every R-module is semisimple.*
(c) *Every R-module is projective.*
(d) *Every R-module is injective.*
(e) *There exist central primitive orthogonal idempotents $e_1, \cdots, e_r \in R$.*
(f) *R is isomorphic to a direct product $R_1 \times \cdots \times R_r$, where each R_i is a two-sided ideal of R, and $R_i \simeq M_{n_i}(D_i)$ for some division ring D_i.*

24. Character Theory

Let G be a finite group, F a field, and (π, V) a finite dimensional representation of G.

Previously when we discussed *characters*, they were homomorphisms $G \to F^\times$. In the context of representation theory, they are called *linear characters* to distinguish from the following.

Definition 24.1. The *character* associated with (π, V) is the function $\chi : G \to F$ given by

$$\chi(g) = \operatorname{tr}(\pi(g)).$$

Linear characters are characters of one-dimensional representations. If χ is the character of (π, V), note that $\chi(e) = \operatorname{tr}(\mathrm{id}) = \dim V$ is the degree of G, as a number in F. If $\operatorname{char}(F) > 0$, $\chi(e)$ may be zero even if $V \neq 0$. On the other hand if $\operatorname{char}(F) = 0$, $\dim V$ is always determined by $\chi(e)$.

From now on we specialize to $F = \mathbb{C}$.

Recall that the trace of an operator $T \in \operatorname{End}(V)$ is invariant under conjugation by $S \in GL(V)$, in other words

$$\operatorname{tr}(T) = \operatorname{tr}(STS^{-1}).$$

Lemma 24.2. *Suppose (π_1, V_1) and (π_2, V_2) are finite dimensional complex representations of G, with associated characters χ_1, χ_2. If V_1 and V_2 are equivalent, then $\chi_1 = \chi_2$.*

Proof. Suppose V_1, V_2 are equivalent, so that there exists an intertwining isomorphism $\phi : V_1 \to V_2$. Then

$$\pi_2(g) \circ \phi = \phi \circ \pi_1(g) \Longrightarrow \pi_2(g) = \phi \circ \pi_1(g) \circ \phi^{-1}$$

hence

$$\chi_2(g) = \operatorname{tr}(\pi_2(g)) = \operatorname{tr}(\phi \circ \pi_1(g) \circ \phi^{-1}) = \operatorname{tr}(\pi_1(g)) = \chi_1(g).$$

□

Therefore the character of a representation is an invariant of its equivalence class.

Definition 24.3. The character χ is called *irreducible* if V is irreducible. The *degree* of χ is that of V.

Suppose that (π, V) is a representation of G, and that $V = V_1 \oplus \cdots \oplus V_n$ is a decomposition into (possibly equivalent) irreducible constituents. If S_i is a basis for V_i, and $S = \coprod_i S_i$. Then for each $g \in G$, the matrix of $\pi(g) \in \mathrm{GL}(V)$ with respect to the basis S will be of the form

$$\left(\begin{array}{c|c|c|c} A_1 & & & \\ \hline & A_2 & & \\ \hline & & \ddots & \\ \hline & & & A_n \end{array}\right)$$

where each A_i is the matrix of $\pi_i(g) \in \mathrm{GL}(V_i)$ with respect to S_i. Then

$$\operatorname{tr}(\pi(g)) = \sum_{i=1}^{n} \operatorname{tr} \pi_i(g) = \operatorname{tr}(\sum_{i=1}^{n} \pi_i(g))$$

which means if χ is the character of V, and χ_i the characters of V_i, then

$$\chi = \sum_{i=1}^{n} \chi_i.$$

We may extend the character $\chi : G \to \mathbb{C}$ to a function $\chi : \mathbb{C}G \to \mathbb{C}$ by linearity:

$$\chi(\sum_g a_g g) = \sum_g a_g \chi(g).$$

Recall from the previous section we have

$$\mathbb{C}G = M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_r}(\mathbb{C})$$

where $M_{n_i}(\mathbb{C}) = \mathrm{End}_{\mathbb{C}G}(V_i)$ as rings, and $M_{n_i}(\mathbb{C}) \simeq V_i^{n_i}$ as $\mathbb{C}G$-modules. Let χ_i be the character of V_i, and e_i be the orthogonal central primitive idempotents that give rise to the above decomposition. On each component $V_j^{n_j} \subset V$, e_i acts by the identity if $i = j$, and by zero otherwise. Then

$$\chi_i(e_i) = n_i, \quad \chi_i(e_j) = 0 \ \text{ for } i \neq j.$$

Lemma 24.4. *The characters $\chi_i : \mathbb{C}G \to \mathbb{C}$ are linearly independent functions.*

Proof. Suppose $\sum_i c_i\chi_i = 0$. Then evaluating on each e_j we get

$$0 = \sum_i c_i\chi_i(e_j) = c_j\chi_j(e_j) = n_jc_j \Longrightarrow c_i = 0.$$

□

Theorem 24.5. *Let V, V' be two finite-dimensional representations of G, with characters χ, χ'. Then V is equivalent to V' if and only if $\chi = \chi'$.*

Proof. We have seen that if V, V' are equivalent, $\chi = \chi'$, so we must prove the converse. Suppose that $V_1, \cdots, V_r$ are distinct irreducible representations of G with characters χ_i, and that

$$V \simeq V_1^{a_1} \oplus \cdots \oplus V_r^{a_r}, \quad V' \simeq V_1^{b_1} \oplus \cdots \oplus V_r^{b_r}.$$

Then

$$\sum_{i=1}^{r} a_i\chi_i = \chi = \chi' = \sum_{i=1}^{r} b_i\chi_i.$$

Since the characters are linearly independent, $a_i = b_i$, hence V, V' are equivalent. □

Definition 24.6. A function $f : G \to \mathbb{C}$ is called a *class function* if $f(g) = f(hgh^{-1})$ for all $h, g \in \mathbb{C}$.

In other words a function $f : G \to \mathbb{C}$ is a class function if and only if f is constant on each conjugacy class $C \subset G$. If G is abelian, any function $f : G \to \mathbb{C}$ is a class function. The sum of two class functions is another one, as is the scalar multiple of a class function, therefore the set $\mathscr{C}(G)$ of all class functions on G is a complex vector space.

Let $\mathbb{C}^G$ denote the set of all complex-valued functions $\eta : G \to \mathbb{C}$. Then $\mathscr{C}(G)$ is a subspace of $\mathbb{C}^G$. We have a bilinear pairing

$$\langle\ ,\ \rangle :\ \mathbb{C}^G \times \mathbb{C}G \to \mathbb{C}, \quad \langle \eta, x\rangle = \eta(x),$$

given explicitly by

$$\langle \eta, \sum_g a_g \cdot g\rangle = \sum_g a_g\eta(g).$$

Proposition 24.7. *The above is a perfect pairing. That is to say, it induces an isomorphism of vector spaces*

$$\mathbb{C}^G \xrightarrow{\sim} \mathbb{C}G^* = \mathrm{Hom}(\mathbb{C}G, \mathbb{C}),$$

where $\eta \in \mathbb{C}^G$ is identified with the functional on $\mathbb{C}G$ given by $\eta(x) = \langle \eta, x\rangle$.

Proof. The map described above is evidently $\mathbb{C}$-linear. Assume that $\eta \in \mathbb{C}^G$ maps to the zero functional under it. Then for each $g \in G$, $0 = \eta(1 \cdot g) = \langle \eta, 1 \cdot g\rangle = \eta(g)$, therefore $\eta \equiv 0$. This shows the map is injective. Since $\dim \mathbb{C}G = \dim G^{\mathbb{C}} = |G|$, it is also surjective. □

The group G acts on $\mathbb{C}G$ (on the left) by conjugation:

$$x = \sum_g a_g \cdot g, \quad h \cdot x = hxh^{-1} = \sum_g a_g hgh^{-1}.$$

It also acts on $\eta \in G^{\mathbb{C}}$ (on the right) by

$$\eta^h(x) = \eta(h \cdot x) = \eta(hxh^{-1}).$$

Therefore

$$\langle \eta, h \cdot x \rangle = \eta(h \cdot x) = \langle \eta^h, x \rangle.$$

Now suppose that $\eta \in G^{\mathbb{C}}$ is a class function, so that for all $h, g \in G$,

$$\eta(g) = \eta(hgh^{-1}) \Longrightarrow \eta(g - hgh^{-1}) = 0.$$

Then $\eta \equiv 0$ on the subspace

$$I = \mathrm{Span}_{\mathbb{C}}\{g - hgh^{-1} : g, h \in G\} \subset \mathbb{C}G.$$

Conversely, any $\eta \in G^{\mathbb{C}}$ that is zero on this subspace is a class function.

Proposition 24.8. (i) *The pairing $\langle\ ,\ \rangle$ induces another perfect pairing*

$$\mathscr{C}(G) \times \mathbb{C}G/I \to \mathbb{C}.$$

(ii) $\mathbb{C}G = Z(\mathbb{C}G) \oplus I$. *In particular,* $\mathbb{Z}(\mathbb{C}G) \simeq \mathscr{C}(G)^*$.

Proof. The first part is just formal, and equivalent to the immediately preceding discussion: since $\eta \in \mathscr{C}(G)$ is zero on $I \subset \mathbb{C}G$, the pairing is well-defined. Since the pairing $\langle\ ,\ \rangle$ is perfect, if η is zero on $\mathbb{C}G/I$, then $\eta \equiv 0$ as an element of $G^{\mathbb{C}}$, hence also of $\mathscr{C}(G)$. This shows we have an injective map $\mathscr{C}(G) \to (\mathbb{C}G/I)^*$. Now given any element of $(\mathbb{C}G/I)^*$, pre-composition with $\mathbb{C}G \to \mathbb{C}G/I$ gives one in $(\mathbb{C}G)^*$ which must come from some $\eta \in G^{\mathbb{C}}$ via the pairing. Then $\eta(I) = 0$ implies $\eta \in \mathscr{C}(G)$, so the map $\mathscr{C}(G) \to (\mathbb{C}G/I)^*$ is also surjective.

Consider the map $T : \mathbb{C}G \to \mathbb{C}G$ given by

$$T(g) = \frac{1}{n} \sum_{h \in G} hgh^{-1}.$$

We claim that T is a projection onto $Z(\mathbb{C}G)$: first note that if $x \in Z(\mathbb{C}G)$, then

$$hxh^{-1} = x \ \text{ for all } h \in G \Longrightarrow T(x) = \frac{1}{n} \sum_{h \in G} x = \frac{1}{n} nx = x,$$

which implies $T(x) = x$. Then from

$$kT(g)k^{-1} = \frac{1}{n} \sum_{h \in G} khgh^{-1}k^{-1} = T(g)$$

it follows that $T(x) \in \mathbb{Z}(\mathbb{C}G)$ for all $x \in \mathbb{C}G$, hence $T(T(x)) = T(x)$, and T is as claimed. Then $\mathbb{C}G = \ker(T) \oplus \mathrm{im}(T)$. We have $T(g - hgh^{-1}) = T(g) - T(g) = 0$, so T vanishes on the generators of I, hence $I \subset \ker(T)$. On the other hand, $\ker(T) = \mathrm{im}(1 - T)$ since T is a projection, and for each $g \in G$, we have

$$(1 - T)(g) = g - \frac{1}{n} \sum_{h \in G} hgh^{-1} = \frac{1}{n} \sum_{h \in G} (g - hgh^{-1}) \in I.$$

This shows $\ker(T) = I$, so $\mathbb{C}G = Z(\mathbb{C}G) \oplus I$. □

Corollary 24.9. $\dim_{\mathbb{C}} \mathscr{C}(G) = \dim_{\mathbb{C}} Z(\mathbb{C}G)$

Theorem 24.10. *The irreducible characters of G form a basis of $\mathscr{C}(G)$. In particular, the number of irreducible representations of G is the same as the number of conjugacy classes in G.*

Proof. Recall that $\mathbb{C}G = M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_r}(\mathbb{C})$. By the Corollary $\dim_{\mathbb{C}} \mathscr{C}(G) = r$. Now $\chi_1, \cdots, \chi_r$ are linearly independent, therefore they must also span $\mathscr{C}(G)$. On the other hand, if $C_1, \cdots, C_m$ are the distinct conjugacy classes in G, then the characteristic functions

$$f_i(g) = \begin{cases} 1 & \text{if } g \in C_i \\ 0 & \text{otherwise} \end{cases}$$

form a basis of $\mathscr{C}(G)$, therefore $m = r$. □

25. Character Orthogonality I

Let G be a finite group, and (π, V) the left-regular representation of G, i.e. $V = \mathbb{C}G$ as a $\mathbb{C}G$-module. Recall the pairing

$$\langle\ ,\ \rangle : \mathbb{C}^G \times \mathbb{C}G \to \mathbb{C}, \quad (\eta, x) = \eta(x) = \sum_{g \in G} a_g \eta(g).$$

For each $\eta \in \mathbb{C}^G$, the map $\widehat{\eta} : \mathbb{C}G \to \mathbb{C}$ defined by $\widehat{\eta}(x) = \langle \eta, x \rangle$ is a linear functional, and

$$\mathbb{C}^G \to (\mathbb{C}G)^*, \quad \eta \mapsto \widehat{\eta}.$$

is a $\mathbb{C}$-linear isomorphism. On the other hand, the vector space $\mathbb{C}G$ has a distinguished basis, namely $\{1 \cdot g : g \in G\}$. Let $\delta_g : \mathbb{C}G \to \mathbb{C}$ be the function

$$\delta_g(\sum_{g \in G} a_g \cdot g) = a_g,$$

so that

$$\mathbb{C}G \to (\mathbb{C}G)^*, \quad g \mapsto \delta_g$$

is a $\mathbb{C}$-linear isomorphism, with inverse

$$(\mathbb{C}G)^* \to \mathbb{C}G, \quad f \mapsto \sum_{g \in G} f(g) \cdot g.$$

Composing the above with $\mathbb{C}^G \to (\mathbb{C}G)^*$ from before we obtain

$$\Phi : \mathbb{C}^G \xrightarrow{\sim} \mathbb{C}G,$$

where

$$\Phi(\eta) = \sum_{g \in G} \langle \eta, g \rangle \cdot g = \sum_{g \in G} \eta(g) \cdot g.$$

Definition 25.1. For $\eta, \nu \in \mathbb{C}^G$, the *convolution* of η and ν is

$$(\eta * \nu)(g) = \sum_{h \in G} \eta(h) \nu(h^{-1} g).$$

Proposition 25.2. *For $\eta, \nu \in \mathbb{C}^G$, $\Phi(\eta * \nu) = \Phi(\eta)\Phi(\nu)$.*

Proof. Since $* : \mathbb{C}^G \times \mathbb{C}^G \to \mathbb{C}^G$ is $\mathbb{C}$-bilinear, it's enough to check the claim for η, ν elements of a particular basis. We do this for the basis $\{\delta_g : g \in G\}$. On the one hand,

$$\Phi(\delta_a) = \sum_{h \in G} \delta_a(h) \cdot h = a,$$

and on the other

$$(\delta_a * \delta_b)(g) = \sum_{h \in G} \delta_a(h) \delta_b(h^{-1} g) = \delta_b(a^{-1} g) = \delta_{ab}(g).$$

Therefore

$$\Phi(\delta_a * \delta_b) = \Phi(\delta_{ab}) = ab = \Phi(\delta_a)\Phi(\delta_b).$$

□

It follows that the convolution product $*$ defines a ring structure on $G^{\mathbb{C}}$, and that $\Phi : \mathbb{C}^G \to \mathbb{C}G$ is a ring isomorphism. Now, recall that $\mathbb{C}G$ decomposes as a ring into

$$\mathbb{C}G = M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_r}(\mathbb{C}).$$

Its center

$$\mathbb{Z}(\mathbb{C}G) = \mathbb{C} \times \mathbb{C} \times \cdots \times \mathbb{C} \quad \text{(r times)}$$

is spanned by

$$e_i = (0, \cdots, 0, 1_{n_i}, 0, \cdots 0),$$

where $1_{n_i} \in M_{n_i}(\mathbb{C})$ is the $n_i \times n_i$ identity matrix. The elements $e_1, \cdots, e_r$ are then central primitive idempotents, satisfying the orthogonality relations

$$(\dagger) \qquad e_i^2 = e_i, \quad e_i e_j = 0 \text{ for } i \neq j.$$

Then via the ring isomorphism $\Phi : \mathbb{C}^G \xrightarrow{\sim} \mathbb{C}G$ the e_i must correspond to idempotents in $\mathbb{C}^G$ which are orthogonal with respect to the convolution product. We will soon see that these are essentially the irreducible characters of G.

Lemma 25.3. *The character χ of the left regular representation of G is*

$$\chi(g) = \begin{cases} |G| & \text{if } g = e \\ 0 & \text{otherwise} \end{cases}$$

Proof. If $g = e$, we have $\chi(g) = \dim \mathbb{C}G = |G|$. We must show $\chi(g) = 0$ if $g \neq e$.

Assume $g \neq e$. Let $\{g_1, \cdots, g_n\}$ be an ordering of G, considered as a basis for $\mathbb{C}G$. Then for each i, $gg_i = g_j$, for some $j \neq i$. Then the matrix of $T_g(x) = gx$ is a permutation matrix with zeros on the diagonal and therefore has trace zero. □

Example 25.4. Let $G = C_3 = \{1, g, g^2\}$. The matrix of $\pi(g)$, resp. $\pi(g^2)$, with respect to the basis $\{1, g, g^2\}$ of $\mathbb{C}G$, is

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \text{resp.} \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

both of which have trace zero.

Corollary 25.5. *For each $x \in \mathbb{C}G$,*

$$x = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}x).$$

By the lemma $\delta_e = |G|^{-1}\chi$. On the other hand,

$$\delta_g(x) = \delta_e(g^{-1}x).$$

For $x = \sum_{g \in G} a_g \cdot g$, we have $\delta_g(x) = a_g$ so

$$x = \sum_{g \in G} \delta_g(x) \cdot g = \sum_{g \in G} \delta_e(g^{-1}x)g = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}x)g.$$

Lemma 25.6. *For each character $\chi : G \to \mathbb{C}$, we have $\chi(g^{-1}) = \overline{\chi(g)}$.*

Proof. Let $g \in G$. Then $g^k = 1$ for some k, since G is finite. Therefore the minimal polynomial of the linear operator $\pi(g)$ divides $X^k - 1$. Since the roots of $X^k - 1$ are distinct, there exists some basis of V in which the matrix of $\pi(g)$ is $\operatorname{diag}(\omega_1, \cdots, \omega_r)$ where ω_i are kth roots of unity. Then $\pi(g^{-1}) = \operatorname{diag}(\omega_1^{-1}, \cdots, \omega_r^{-1}) = \operatorname{diag}(\overline{\omega_1}, \cdots, \overline{\omega_r})$ so

$$\chi(g^{-1}) = \operatorname{tr} \pi(g^{-1}) = \overline{\operatorname{tr} \pi(g)} = \overline{\chi(g)}.$$

□

Let $\chi_1, \cdots, \chi_r$ be the irreducible characters of G, corresponding to the decomposition

$$\mathbb{C}G = n_1 V_1 \oplus \cdots \oplus n_r V_r$$

of the left regular representation.

Lemma 25.7. *We have $\Phi(\chi_i^*) = e_i$, where*

$$\chi_i^*(g) = \frac{n_i}{|G|}\overline{\chi_i}.$$

Proof. Setting $x = e_i$ in the corollary, we obtain

$$e_i = \frac{1}{|G|}\sum_{g\in G} \chi(g^{-1}e_i)g.$$

Now $\chi = \sum_i n_i\chi_i$ implies

$$\chi(ge_i) = \sum_j n_j\chi_j(ge_i) = n_i\chi_i(ge_i) = n_i\chi_i(g).$$

Then using the previous lemma,

$$e_i = \frac{n_i}{|G|}\sum_{g\in G}\chi_i(g^{-1})g = \sum_{g\in G}\left(\frac{n_i}{|G|}\overline{\chi_i(g)}\right)\cdot g = \Phi(\chi_i^*).$$

□

Corollary 25.8. *We have*

$$\frac{n_i}{|G|}\chi_i * \chi_i = \chi_i, \quad \chi_i * \chi_j = 0, \quad \textit{for } i \neq j.$$

Proof. Using the lemma, Proposition 25.2, and the relations (†), we have

$$\chi_i^* * \chi_j^* = \Phi(e_i) * \Phi(e_j) = \Phi(e_ie_j) = \begin{cases} \Phi(e_i) = \chi_i^* & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Substituting the expression for χ_i^* we get

$$\frac{n_i}{|G|}\overline{\chi}_i = \chi_i^* * \chi_i^* = (\frac{n_i}{|G_i|}\overline{\chi}_i) * (\frac{n_i}{|G|}\overline{\chi}_i) = \frac{n_i^2}{|G|^2}\overline{\chi}_i * \overline{\chi}_i \Longrightarrow \frac{n_i}{|G|}\chi_i * \chi_i = \chi_i,$$

since $\overline{\eta} * \overline{\nu} = \overline{\eta * \nu}$. □

Next we will show that the so-called first and second character orthogonality relations follow from the above corollary.

26. Character Orthogonality II

Recall that $\chi_1, \cdots, \chi_r$ form a basis for the vector space $\mathscr{C}(G)$ of class functions on G. We will prove that $\chi_1, \cdots, \chi_r$ are in fact orthonormal, with respect to a hermitian form on $\mathscr{C}(G)$ that we now define.

Let $\iota : G \to G$ be the inverse map $\iota(g) = g^{-1}$. We also write $\iota : \mathbb{C}G \to \mathbb{C}G$ for the $\mathbb{C}$-linear map induced by it. Let

$$\epsilon : \mathbb{C}G \to \mathbb{C}, \quad \epsilon(\sum_{g\in G} a_g \cdot g) = a_e$$

and define a pairing $(\ ,\ ) : \mathbb{C}G \times \mathbb{C}G \to \mathbb{C}$ by

$$(x, y) = \epsilon(x \cdot \iota(y)).$$

It's a homework exercise to check that this is a non-degenerate bilinear form on $\mathbb{C}G$. Explicitly, for

$$x = \sum_{g\in G} a_g \cdot g, \quad y = \sum_{g\in G} b_g \cdot g,$$

we have

$$(x, y) = \epsilon(\sum_{g,h} a_g b_h g h^{-1}) = \sum_{g\in G} a_g b_{g^{-1}}.$$

We also define

$$(\ ,\ ) : \mathbb{C}^G \to \mathbb{C}^G \to \mathbb{C}$$

by

$$(\eta, \nu) = (\eta * \iota(\nu))(e) = \sum_{h\in G} \eta(h)\nu(h^{-1}).$$

The use of the same symbol $(\ ,\ )$ is justified by the following.

Lemma 26.1. *The map $\Phi : \mathbb{C}^G \to \mathbb{C}G$ preserves the bilinear forms, i.e.*

$$(\Phi(\eta), \Phi(\nu)) = (\eta, \nu), \quad \eta, \nu \in \mathbb{C}^G.$$

Proof. Exercise. □

Definition 26.2. Let $H : \mathscr{C}(G) \times \mathscr{C}(G) \to \mathbb{C}$ be the hermitian form

$$H(\alpha, \beta) = \frac{1}{|G|} \sum_{g\in G} \alpha(g)\overline{\beta(g)}.$$

Theorem 26.3 (First Character Orthogonality Relation)**.** *The characters χ_i are orthonormal with respect to H on $\mathbb{C}^G$. In other words, for $i \neq j$,*

$$\frac{1}{|G|} \sum_{g\in G} |\chi_i(g)|^2 = 1, \quad \sum_{g\in G} \chi_i(g)\overline{\chi_j(g)} = 0.$$

Proof. By Corollary 25.8 for $i \neq j$ we have,

$$\frac{n_i}{|G|}\chi_i * \chi_i = \chi_i, \quad \chi_i * \chi_j = 0$$

It follows that for $i \neq j$,

$$\chi_i * \chi_j = 0 \Longrightarrow (\chi_i, \chi_j) = 0$$

and that

$$\frac{n_i}{|G|}(\chi_i, \chi_i) = \chi_i(e) = n_i \Longrightarrow \frac{1}{|G|}(\chi_i, \chi_i) = 1.$$

Now for any characters χ_i, χ_j,

$$H(\chi_i, \chi_j) = \frac{1}{|G|} \sum_{g\in G} \chi_i(g)\overline{\chi_j}(g) = \frac{1}{|G|} \sum_{g\in G} \chi_1(g)\chi_2(g^{-1}) = \frac{1}{|G|}(\chi_i * \chi_j)(e) = \frac{1}{|G|}(\chi_i, \chi_j).$$

□

Let $C_1, \cdots, C_r$ be the distinct conjugacy classes of G, and choose $g_i \in C_i$. We assume C_1 is the trivial conjugacy class, so that $g_1 = e$. Since characters are class functions, each character χ_i is completely determined by the values $\chi_i(g_1), \cdots, \chi_i(g_r)$.

Definition 26.4. The matrix $(\chi_i(g_j))$ is called the *character table* of G.

Note that the character table is a square matrix. Since each irreducible representation of G is completely determined by its character, the character table is a summary of the possible representations of G.

Example 26.5. The character table of S_3 is

$$\begin{pmatrix} 1 & -1 & 1 \\ 2 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix}.$$

The rows correspond to the irreducible characters χ_1, χ_2, χ_3. The columns correspond to conjugacy classes C_1, C_2, C_3. Since $C_1 = \{e\}$, and $\chi_i(e) = \deg \chi_i$, the first column (on the left) is the list of degrees. Therefore χ_1, χ_3 have degree 1, and correspond to linear characters. Since the last row is all 1s, χ_3 is the trivial character, so χ_1 must be the sign character. The second column therefore corresponds to the conjugacy class of transpositions.

The second row corresponds to the unique irreducible character χ_2 of S_3 with degree 2, which is the standard representation introduced before. Recall that it's the action of S_3 on $\{(z_1, z_2, z_3) : z_1 + z_2 + z_3 = 0\}$, which is spanned by $\alpha = (1, 0, -1)$ and $\beta = (1, -1, 0)$.

Choosing $g_2 = (12)$, $g_3 = (123) \in S_3$ to represent the conjugacy class of transpositions and 3-cycles we have

$$g_2 \cdot \alpha = (0, 1, -1) = \alpha - \beta, \qquad g_2 \cdot \beta = (-1, 1, 0) = -\beta.$$
$$g_3 \cdot \alpha = (0, -1, 1) = \beta - \alpha, \qquad g_3 \cdot \beta = (-1, 0, 1) = -\alpha$$

If $g_1 = (1)$, the matrix of g_1, g_2, g_3 with respect to $\{\alpha, \beta\}$ is

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}.$$

Taking the traces, we obtain the values of χ_2 on (g_1, g_2, g_3), which are indeed $(2, 0, -1)$.

Example 26.6. The character table of the cyclic group of order 4 is

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \\ 1 & -i & -1 & -i \end{pmatrix}.$$

For an abelian group, all irreducible characters are linear, and all conjugacy classes have only one element. Then the columns of this matrix simply correspond to the elements $\{1, g, g^2, g^3\}$ of the group, and the rows are $\chi(1), \chi(g), \chi(g)^2, \chi(g)^3$. The third row corresponds to the character determined by $\chi_0(g) = i$, and the other three are χ_0^k for $k = 2, 3, 4$.

Let $g_1, \cdots, g_r$ represent the conjugacy classes $C_1, \cdots, C_r$ of a finite group G, and $\chi_1, \cdots, \chi_r$ the irreducible conjugacy classes. By the first character orthogonality relation

$$\delta_{ij} = \frac{1}{|G|} \sum_{g \in G} \chi_i(g) \overline{\chi}_j(g) = \frac{1}{|G|} \sum_{k=1}^{r} \sum_{g \in C_k} \chi_i(g_k) \overline{\chi}_j(g_k) = \sum_{k=1}^{r} \frac{|C_k|}{|G|} \chi_i(g_k) \overline{\chi}_j(g_k).$$

Now C_k is the orbit of g_k under the action of G by conjugation. By the orbit stabilizer-theorem, $\frac{|G|}{|C_k|} = |C_G(g_k)|$, the order of the centralizer of g_k in G. Then

$$\delta_{ij} = \sum_{k=1}^{r} \frac{1}{|C_G(g_k)|} \chi_i(g_k) \overline{\chi}_j(g_k)$$

Let $X = (\chi_i(g_j))$ be the character table of G, and $X^* = (\overline{\chi}_j(g_i))$ its conjugate transpose. Let $D = \operatorname{diag}(|C_G(g_1)|, \cdots, |C_G(g_r)|)$. Then the relation above can be written as

$$1 = X D^{-1} X^*,$$

which says $D^{-1}X^*$ is the right-inverse of X. Therefore, it's also the left-inverse of X, so

$$1 = D^{-1} X^* X \iff D = X^* X.$$

In terms of the matrix entries,

$$|C_G(g_i)|\delta_{ij} = \sum_{k=1}^{r} X_{ik}^* X_{kj} = \sum_{k=1}^{r} \overline{\chi}_k(g_i)\chi_k(g_j).$$

We have therefore proven:

Theorem 26.7 (Second Orthogonality Relation)**.** *For $g, h \in G$,*

$$\sum_{g\in G} \chi_i(g)\overline{\chi_i}(h) = \begin{cases} |C_G(g)| & \text{if } g, h \text{ are conjugate.} \\ 0 & \text{otherwise.} \end{cases}$$