MATH457 - Algebra 4

Representation Theory; Galois Theory

Based on lectures from Winter 2025 by Prof. Henri Darmon.
Notes by Louis Meunier

Contents

§1 Representation Theory

Recall that in studying group theory, we studied the notation of a group "acting" on a set. Representation theory studies group actions on vector spaces, which takes the notion of a group action on a set, and makes it compatible with the vector space structure.

§1.1 Introduction

↪**Definition 1.1** (Linear Representation): A *linear representation* of a group G is a vector space V over a field $\mathbb{F}$ equipped with a map $G \times V \to V$ that makes V a G-set in such a way that for each $g \in G$, the map $v \mapsto gv$ is a linear homomorphism of V.

This induces a homomorphism

$$\rho : G \to \mathrm{Aut}_{\mathbb{F}}(V),$$

or, in particular, when $n = \dim_{\mathbb{F}} V < \infty$, a homomorphism

$$\rho : G \to \mathrm{GL}_n(\mathbb{F}).$$

Alternatively, a linear representation V can be viewed as a module over the group ring $\mathbb{F}[G] = \left\{\sum_{g\in G} : \lambda_g g : \lambda_g \in \mathbb{F}\right\}$ (where we require all but finitely many scalars λ_g to be zero).

↪**Definition 1.2** (Irreducible Representation): A linear representation V of a group G is called *irreducible* if there exists no proper, nontrivial *subspace* $W \subsetneq V$ such that W is G-stable.

⊛ **Example 1.1**:

1. Consider $G = \mathbb{Z}/2 = \{1, \tau\}$. If V a linear representation of G and $\rho : G \to \mathrm{Aut}(V)$. Then, V uniquely determined by $\rho(\tau)$. Let $p(x)$ be the minimal polynomial of $\rho(\tau)$. Then, $p(x) \mid x^2 - 1$. Suppose $\mathbb{F}$ is a field in which $2 \neq 0$. Then, $p(x) \mid (x-1)(x+1)$ and so $p(x)$ has either $1, -1$, or both as eigenvalues and thus we may write

   $$V = V_+ \oplus V_-,$$

   where $V_\pm := \{v \mid \tau v = \pm v\}$. Hence, V is irreducible only if one of V_+, V_- all of V and the other is trivial, or in other words τ acts only as multiplication by 1 or -1.
2. Let $G = \{g_1, \ldots, g_N\}$ be a finite abelian group, and suppose $\mathbb{F}$ an algebraically closed field of characteristic 0 (such as $\mathbb{C}$). Let $\rho : G \to \mathrm{Aut}\,(V)$ and denote $T_j := \rho\left(g_j\right)$ for $j = 1, \ldots, N$. Then, $\{T_1, \ldots, T_N\}$ is a set of mutually commuting linear transformations. Then, there exists a simultaneous eigenvector, say v, for $\{T_1, \ldots, T_N\}$, and so span (v) a G-stable subspace of V. Thus, if V irreducible, it must be that $\dim_{\mathbb{F}} V = 1$.

↪**Theorem 1.1**: If G a finite abelian group and V an irreducible finite dimensional representation over an algebraically closed field of characteristic 0, then $\dim V = 1$.

Proof. Let $\rho : G \to \mathrm{Aut}(V)$, label $G = \{g_1, ..., g_N\}$ and put $T_j := \rho\left(g_j\right)$ for $j = 1, ..., N$. Then, $\{T_1, ..., T_N\}$ a family of mutually commuting linear transformations on V. Then, there is a simultaneous eigenvector v for $\{T_1, ..., T_N\}$ and thus $\mathrm{span}(v)$ is $T_1, ..., T_N$-stable and so $V = \mathrm{span}(v)$. ■

↪**Lemma 1.1**: Let V be a finite dimensional vector space over $\mathbb{C}$ and let $T_1, ..., T_N : V \to V$ be a family of mutually commuting linear automorphisms on V. Then, there is a simultaneous eigenvector for $T_1, ..., T_N$.

↪**Proposition 1.1**: Let $\mathbb{F}$ a field where $2 \neq 0$ and V an irreducible representation of S_3. Then, there are three distinct (i.e., up to homomorphism) possibilities for V.

Proof. Let $\rho : G \to \mathrm{Aut}(V)$ and let $T = \rho((23))$. Then, notice that $p_T(x) \mid \left(x^2 - 1\right)$ so T has eigenvalues in $\{-1, 1\}$.

If the only eigenvalue of T is -1, we claim that V one-dimensional.

If T has 1 as an eigenvalue. ■

↪**Proposition 1.2**: D_8 has a unique faithful irreducible representation, of dimension 2 over a field F in which $0 \neq 2$.

Proof. Write $G = D_8 = \left\{1, r, r^2, r^3, v, h, d_1, d_2\right\}$ as standard. Let ρ be our irreducible, faithful representation and let $T = \rho\left(r^2\right)$. Then, $p_T(x) \mid x^2 - 1 = (x-1)(x+1)$ and so $V = V_+ \oplus V_-$, the respective eigenspaces for $\lambda = +1, -1$ respectively for T. Then, notice that since r^2 in the center of G, both V_+ and V_- are preserved by the action of G, hence one must be trivial and the other the entirety of V. V can't equal V_+, else $T = I$ on all of V hence ρ not faithful so $V = V_-$.

Next, it must be that $\rho(h)$ has both eigenvalues 1 and -1. Let $v_1 \in V$ be such that $hv_1 = v_1$ and $v_2 = rv_1$. We claim that $W := \mathrm{span}\ \{v_1, v_2\}$, namely $V = W$ 2-dimensional.

We simply check each element. $rv_1 = v_2$ and $rv_2 = r^2 v_1 = -v_1$ which are both in W hence r and thus $\langle r \rangle$ fixes W. Next, $hv_1 = v_1$ and $vv_2 = vrv_1 = rhv_1 = rv_1 = v_2$ (since $rhr^{-1} = v$) and so $hv_2 = -v_2$ and $vv_1 = -v_1$ and so W G-stable. Finally, d_1 and d_2 are just products of these elements and so W G-stable. ■

↪**Definition 1.3** (Isomorphism of Representations): Given a group G and two representations $\rho_i : G \to \mathrm{Aut}_{\mathbb{F}}(V_i)$, $i = 1, 2$ an isomorphism of representations is a vector space isomorphism $\varphi : V_1 \to V_2$ that respects the group action, namely

$$\varphi(gv) = g\varphi(v)$$

for every $g \in G, v \in V_1$.

§1.2 Maschke's Theorem

↪**Theorem 1.2** (Maschke's): Any representation of a finite group G over $\mathbb{C}$ can be written as a direct sum of irreducible representations, i.e.

$$V = V_1 \oplus \cdots \oplus V_t,$$

where V_j irreducible.

Remark 1.1: $|G| < \infty$ essential. For instance, consider $G = (\mathbb{Z}, +)$ and 2-dimensional representation given by $n \mapsto \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$. Then, $n \cdot e_1 = e_1$ and $n \cdot e_2 = ne_1 + e_2$. We have that $\mathbb{C}e_1$ irreducible then. But if $v = ae_1 + e_2 \in W := V \setminus \mathbb{C}e_1$, then $Gv = (a+1)e_1 + e_2$ so $Gv - v = e_1 \in W$, contradiction.

Remark 1.2: $|\mathbb{C}|$ essential. Suppose $F = \mathbb{Z}/3\mathbb{Z}$ and $V = Fe_1 \oplus Fe_2 \oplus Fe_3$, and $G = S_3$ acts on V by permuting the basis vectors e_i. Then notice that $F(e_1 + e_2 + e_3)$ an irreducible subspace in V. Let $W = F(w)$ with $w := ae_1 + be_2 + ce_3$ be any other G-stable subspace. Then, by applying (123) repeatedly to w and adding the result, we find that $(a+b+c)(e_1 + e_2 + e_3) \in W$. Similarly, by applying $(12), (23), (13)$ to w, we find $(a-b)(e_1 - e_2), (b-c)(e_2 - e_3), (a-c)(e_1 - e_3)$ all in W. It must be that at least one of $a-b, a-c, b-c$ nonzero, else we'd have $w \in F(e_1 + e_2 + e_3)$. Assume wlog $a - b \neq 0$. Then, we may apply $(a-b)^{-1}$ and find $e_1 - e_2 \in W$. By applying $(23), (13)$ to this vector and scaling, we find further $e_2 - e_3$ and $e_1 - e_3 \in W$. But then,

$$2(e_1 - e_2) + 2(e_1 - e_3) = e_1 + e_2 + e_3 \in W,$$

so $F(e_1 + e_2 + e_3)$ a subspace of W, a contradiction.

↪**Proposition 1.3**: Let V be a representation of $|G| < \infty$ over $\mathbb{C}$ and let $W \subseteq V$ a sub-representation. Then, W has a G-stable complement W', such that $V = W \oplus W'$.

Proof. Denote by ρ the homomorphism induced by the representation. Let $W_{0'}$ be any complementary subspace of W and let

$$\pi : V \to W$$

be a projection onto W along $W_{0'}$, i.e. $\pi^2 = \pi, \pi(V) = W$, and $\ker(\pi) = W_{0'}$. Let us "replace" π by the "average"

$$\tilde{\pi} := \frac{1}{\#G} \sum_{g \in G} \rho(g)\pi\rho(g)^{-1}.$$

Then the following hold:

(1) $\tilde{\pi}$ G-equivariant, that is $\tilde{\pi}(gv) = g\tilde{\pi}(v)$ for every $g \in G, v \in V$.

(2) $\tilde{\pi}$ a projection onto W.

Let $W' = \ker(\tilde{\pi})$. Then, W' G-stable, and $V = W \oplus W'$. ■

We present an alternative proof to the previous proposition by appealing to the existence of a certain inner product on complex representations of finite groups.

↪**Definition 1.4**: Given a vector space V over $\mathbb{C}$, a *Hermitian pairing/inner product* is a hermitian-bilinear map $V \times V \to \mathbb{C}$, $(v, w) \mapsto \langle v, w \rangle$ such that

- linear in the first coordinate;
- conjugate-linear in the second coordinate;
- $\langle v, v \rangle \in \mathbb{R}^{\geq 0}$ and equal to zero iff $v = 0$.

↪**Theorem 1.3**: Let V be a finite dimensional complex representation of a finite group G. Then, there is a hermitian inner product $\langle \cdot, \cdot \rangle$ such that $\langle gv, gw \rangle = \langle v, w \rangle$ for every $g \in G$ and $v, w \in V$.

Proof. Let $\langle \cdot, \cdot \rangle_0$ be any inner product on V (which exists by defining $\langle e_i, e_j \rangle_0 = \delta_i^j$ and extending by conjugate linearity). We apply "averaging":

$$\langle v, w \rangle := \frac{1}{\#G} \sum_{g \in G} \langle gv, gw \rangle.$$

Then, one can check that $\langle \cdot, \cdot \rangle$ is hermitian linear, positive, and in particular G-equivariant. ■

From this, the previous proposition follows quickly by taking $W' = W^{\perp}$, the orthogonal complement to W with respect to the G-invariant inner product that the previous theorem provides.

From this proposition, Maschke's follows by repeatedly applying this logic. Since at each stage V is split in two, eventually the dimension of the resulting dimensions will become zero since V finite dimensional. Hence, the remaining vector spaces $V_1, \ldots, V_t$ left will necessarily be irreducible, since if they weren't, we could apply the proposition further.

↪**Theorem 1.4** (Schur's Lemma): Let V, W be irreducible representations of a group G. Then,

$$\mathrm{Hom}_G(V,W) = \begin{cases} 0 \text{ if } V \underset{G}{\not\cong} W \\ \mathbb{C} \text{ if } V \underset{G}{\cong} W \end{cases},$$

where $\mathrm{Hom}_G(V,W) = \{T : V \to W \mid T \text{ linear and } G-\text{equivariant}\}$.

Proof. Suppose $V \underset{G}{\not\cong} W$ and let $T \in \mathrm{Hom}_G(V,W)$. Then, notice that $\ker(T)$ a subrepresentation of V (a subspace that is a representation in its own right), but by assumption V irreducible hence either $\ker(T) = V$ or $\{0\}$.

If $\ker(T) = V$, then T trivial, and if $\ker(T) = \{0\}$, then this implies $T : V \to \mathrm{im}(T) \subset W$ a representation isomorphism, namely $\mathrm{im}(T)$ a irreducible subrepresentation of W. This implies that, since W irreducible, $\mathrm{im}(T) = W$, contradicting the original assumption.

Suppose now $V \underset{G}{\cong} W$. Let $T \in \mathrm{Hom}_G(V,W) = \mathrm{End}_G(V)$. Since $\mathbb{C}$ algebraically closed, T has an eigenvalue, λ. Then, notice that $T - \lambda I \in \mathrm{End}_G(V)$ and so $\ker(T - \lambda I) \subset V$ a, necessarily trivial because V irreducible, subrepresentation of V. Hence, $T - \lambda I = 0 \Rightarrow T = \lambda I$ on V. It follows that $\mathrm{Hom}_G(V,W)$ a one-dimensional vector space over $\mathbb{C}$, so namely $\mathbb{C}$ itself. ■

↪**Corollary 1.1**: Given a general representation $V = \bigoplus_{j=1}^{t} V_j^{m_j}$,

$$m_j = \dim_{\mathbb{C}} \mathrm{Hom}_G\big(V_j, V\big).$$

↪**Definition 1.5** (Trace): The trace of an endomorphism $T : V \to V$ is the trace of any matrix defining T. Since the trace is conjugation-invariant, this is well-defined regardless of basis.

↪**Proposition 1.4**: Let $W \subseteq V$ a subspace and $\pi : V \to W$ a projection. Then, $\mathrm{tr}(\pi) = \dim(W)$.

↪**Theorem 1.5**: If $\rho : G \to \mathrm{Aut}_{\mathbb{F}}(V)$ a complex representation of G, then

$$\dim\big(V^G\big) = \frac{1}{\#G} \sum_{g \in G} \mathrm{tr}(\rho(g)),$$

where $V^G = \{v \in V : gv = v \,\forall\, g \in G\}$.

Proof. Let $\pi = \frac{1}{\#G} \sum_{g \in G} \rho(g)$. Then,

$$\pi^2 = \left(\frac{1}{\#G}\right)^2 \sum_{g\in G}\sum_{h\in G} \rho(gh)$$
$$= \left(\frac{1}{\#G}\right)^2 \#G \sum_{g\in G} \rho(g) = \pi.$$

We show $V^G = \mathrm{im}(\pi)$. If $v \in \mathrm{im}(\pi)$, then $v = \pi(w)$, so for every $h \in G$,

$$\rho(h)v = \frac{1}{\#G}\sum_{g\in G}\rho(hg)w$$
$$= \frac{1}{\#G}\sum_{hg\in G}\rho(hg)w$$
$$= \pi(w) = v,$$

so $v \in V^G$. Conversely, if $v \in V^G$, then

$$\pi(v) = \frac{1}{\#G}\sum_{g\in G}\rho(g)v = \frac{1}{\#G}\sum_{g\in G} v = v,$$

so $v \in \mathrm{im}(\pi)$. Hence, π a projection with image V^G, so we conclude

$$\dim\left(V^G\right) = \mathrm{tr}(\pi) = \frac{1}{\#G}\sum_{g\in G}\mathrm{tr}(\rho(g)).$$

■

§1.3 Characters, Orthogonality, Number of Irreducible Representations

↪**Definition 1.6**: Let $\dim(V) < \infty$ and G a group. The *character* of V is the function

$$\chi_V : G \to \mathbb{C}, \qquad \chi_V(g) := \mathrm{tr}(\rho(g)).$$

↪**Proposition 1.5**: Characters are class functions, namely constant on conjugacy classes.

Proof. Follows from the fact that the trace of a matrix is conjugation invariant. ■

↪**Proposition 1.6**: Given two representations V, W of G, there is a natural action of G on $\mathrm{Hom}(V,W)$ given by $g * T = g \circ T \circ g^{-1}$. Then,

$$\mathrm{Hom}(V,W)^G = \{T : V \to W \mid g * T = T\},$$

so

$$\mathrm{Hom}(V,W)^G = \mathrm{Hom}_G(V,W).$$

↪**Proposition 1.7**: Suppose $V = V_1^{m_1} \oplus \cdots \oplus V_t^{m_t}$ a representation of G written in irreducible form. Then,

$$\mathrm{Hom}_G\big(V_j, V\big) = \mathbb{C}^{(m_)j}.$$

Proof. By Maschke's Theorem and Schur's Lemma combined,

$$\begin{aligned}\mathrm{Hom}_G\big(V_j, V\big) &= \mathrm{Hom}_G\big(V_j, V_1^{m_1} \oplus \cdots \oplus V_t^{m_t}\big)\\ &= \bigoplus_{i=1}^{t} \mathrm{Hom}_G\big(V_j, V_i\big)^{m_i}\\ &= \mathbb{C}^{m_j}\end{aligned}$$

■

↪**Proposition 1.8**: If V, W are two representations, then so is $V \oplus W$ with point-wise action, and $\chi_{V\oplus W} = \chi_V + \chi_W$.

Proof. We may pick an appropriate basis for $g \in G$ such that g acts on $V \oplus W$ as

$$g = \begin{pmatrix} [\rho_V(g)] & 0 \\ 0 & \big[\rho_{W(g)}\big] \end{pmatrix},$$

where ρ_V, ρ_W are the matrix representations of g acting on V, W respectively. From this, it is immediate that $\mathrm{tr}(g) = \mathrm{tr}(\rho_V(g)) + \mathrm{tr}(\rho_W(g)) = \chi_V + \chi_W$. ■

↪**Theorem 1.6**: $\chi_{\mathrm{Hom}(V,W)} = \overline{\chi_V}\chi_W$.

Proof. Let $g \in G$ and $e_1, \ldots, e_n$ an eigenbasis for V such that $ge_i = \lambda_i e_i$ and $f_1, \ldots, f_m$ an eigenbasis for W such that $gf_j = \mu_j f_j$. Then,

$$\Big\{\varphi_i^j : V \to W \mid \varphi_i^j(e_\ell) = f_j \cdot \delta_i^\ell, 1 \le i \le n, 1 \le j \le m\Big\}$$

is a basis for $\mathrm{Hom}(V, W)$, upon which g acts by

$$\begin{aligned} g\varphi_i^j(g^{-1}e_\ell) &= g\varphi_i^j\big(\lambda_\ell^{-1}e_\ell\big)\\ &= \lambda_\ell^{-1} g f_j \delta_i^\ell\\ &= \lambda_\ell^{-1}\mu_j\delta_i^\ell,\end{aligned}$$

hence

$$\mathrm{tr}(g) = \left(\sum_{i=1}^{n}\lambda_\ell^{-1}\right)\left(\sum_{j=1}^{m}\mu_j\right) = \left(\sum_{i=1}^{n}\overline{\lambda_i}\right)\left(\sum_{j=1}^{m}\mu_j\right) = \left(\overline{\sum_{i=1}^{n}\lambda_i}\right)\left(\sum_{j=1}^{m}\mu_j\right) = \overline{\chi_V(g)}\chi_W(g)$$

where we use the fact that $\lambda^{-1} = \overline{\lambda}$ being a root of unity, and complex conjugation is linear. ■

↪**Theorem 1.7** (Orthogonality of Irreducible Group Characters): Suppose $V_1, \dots, V_t$ is a list of irreducible representations of G and $\chi_1, \dots, \chi_t$ are their corresponding characters. Then, the χ_j's naturally live in the space $L^2(G) \simeq \mathbb{C}^{\#G}$, which we can equip with the inner product

$$\langle f_1, f_2 \rangle : \frac{1}{\#G} \sum_{g \in G} \overline{f_1(g)} f_2(g).$$

Then,

$$\langle \chi_i, \chi_j \rangle = \delta_i^j.$$

Proof.

$$\begin{aligned}
\langle \chi_i, \chi_j \rangle &= \frac{1}{\#G} \sum_{g \in G} \overline{\chi_i(g)} \chi_j(g) \\
&= \frac{1}{\#G} \sum_{g \in G} \chi_{\mathrm{Hom}\left(V_i, V_j\right)}(g) \\
&= \dim_{\mathbb{C}} \left(\mathrm{Hom}\left(V_i, V_j\right)^G \right) \\
&= \begin{cases} \dim_{\mathbb{C}}(\mathbb{C}) i = j \\ \dim_{\mathbb{C}}(0) i \neq j \end{cases} = \delta_i^j.
\end{aligned}$$

■

↪**Corollary 1.2**: $\chi_1, \dots, \chi_t$ orthonormal vectors in $L^2(G)$.

↪**Corollary 1.3**: $\chi_1, \dots, \chi_t$ linearly independent, so in particular $t \leq \#G = \dim L^2(G)$.

↪**Corollary 1.4**: $t \leq h(G) :=$ # conjugacy classes.

Proof. We have that $L_c^2(G) \subseteq L^2(G)$, where $L_c^2(G)$ is the space of $\mathbb{C}$-valued functions on G that are constant on conjugacy classes. It's easy to see that $\dim_{\mathbb{C}}\left(L_c^2(G)\right) = h(G)$. Then, since $\chi_1, \dots, \chi_t$ are class functions, the live naturally in $L_c^2(G)$ and hence since they are linearly independent, there are at most $h(G)$ of them. ■

Remark 1.3: We'll show this inequality is actually equality soon.

↪**Theorem 1.8** (Characterization of Representation by Characters): If V, W are two complex representations, they are isomorphic as representations $\Leftrightarrow \chi_V = \chi_W$.

PROOF. By Maschke's, $V = V_1^{m_1} \oplus \cdots \oplus V_t^{m_t}$ and hence $\chi_V = m_1\chi_1 + \cdots + m_t\chi_t$. By orthogonality, $m_j = \langle \chi_V, \chi_j \rangle$ for each $j = 1, \ldots, t$, hence V completely determined by χ_V. ■

↪**Definition 1.7** (Regular Representation): Define

$$\begin{aligned} V_{\text{reg}} &:= \mathbb{C}[G] \text{ with left mult.} \\ &\simeq L^2(G) \text{ with } (g * f)(x) := f\left(g^{-1}x\right), \end{aligned}$$

the "regular representation" of G.

↪**Proposition 1.9**: $\chi_{\text{reg}}(g) = \begin{cases} \#G & \text{if } g = \text{id} \\ 0 & \text{else} \end{cases}$.

PROOF. If $g = \text{id}$, then g simply acts as the identity on V_{reg} and so has trace equal to the dimension of V_{reg}, which has as basis just the elements of G hence dimension equal to $\#G$. If $g \neq \text{id}$, then g cannot fix any basis vector, i.e. any other element $h \in G$, since $gh = h \Leftrightarrow g = \text{id}$. Hence, g permutes every element in G with no fixed points, hence its matrix representation in the standard basis would have no 1s on the diagonal hence trace equal to zero. ■

↪**Theorem 1.9**: Every irreducible representation of V, V_j, appears in V_{reg} at least once, specifically, with multiplicity $\dim_{\mathbb{C}}\left(V_j\right)$. Specifically,

$$V_{\text{reg}} = V_1^{d_1} \oplus \cdots \oplus V_t^{d_t},$$

where $d_j := \dim_{\mathbb{C}}\left(V_j\right)$.

In particular,

$$\#G = d_1^2 + \cdots + d_t^2.$$

PROOF. Write $V_{\text{reg}} = V_1^{m_1} \oplus \cdots \oplus V_t^{m_t}$. We'll show $m_j = d_j$ for each $j = 1, \ldots, t$. We find

$$\begin{aligned} m_j &= \langle \chi_{\text{reg}}, \chi_j \rangle \\ &= \frac{1}{\#G} \sum_{g \in G} \overline{\chi_{\text{reg}}(g)} \chi_j(g) \\ &= \frac{1}{\#G} \#G \chi_j(\text{id}) = \chi_j(\text{id}) = d_j, \end{aligned}$$

since the trace of the identity element acting on a vector space is always the dimension of the space. In particular, then

$$\begin{aligned}\#G = \dim_{\mathbb{C}}\left(V_{\text{reg}}\right) &= \dim_{\mathbb{C}}\left(V_1^{d_1} \oplus \cdots \oplus V_t^{d_t}\right) \\ &= d_1 \cdot \dim_{\mathbb{C}}(V_1) + \cdots + d_t \cdot \dim_{\mathbb{C}}(V_t) \\ &= d_1^2 + \cdots + d_t^2.\end{aligned}$$

■

↪**Theorem 1.10**: $t = h(G)$.

Proof. Remark that $\mathbb{C}[G]$ has a natural ring structure, combining multiplication of coefficients in $\mathbb{C}$ and internal multiplication in G. Define a group homomorphism

$$\underline{\rho} = (\rho_1, \ldots, \rho_t) : G \to \text{Aut}(V_1) \times \cdots \times \text{Aut}(V_t),$$

collecting all the irreducible representation homomorphisms into a single vector. Then, this extends naturally by ($\mathbb{C}$-)linearity to a ring homomorphism

$$\underline{\rho} : \mathbb{C}[G] \to \text{End}_{\mathbb{C}}(V_1) \oplus \cdots \oplus \text{End}_{\mathbb{C}}(V_t).$$

By picking bases for each $\text{End}_{\mathbb{C}}\left(V_j\right)$, we find that $\dim_{\mathbb{C}}\left(\text{End}_{\mathbb{C}}\left(V_j\right)\right) = d_j^2$ hence $\dim_{\mathbb{C}}(\text{End}_{\mathbb{C}}(V_1) \oplus \cdots \oplus \text{End}_{\mathbb{C}}(V_t)) = d_1^2 + \cdots + d_t^2 = \#G$, as we saw in the previous theorem. On the other hand, $\dim_{\mathbb{C}}(\mathbb{C}[G]) = \#G$ hence the dimensions of the two sides are equal. We claim that $\underline{\rho}$ an isomorphism of rings. By dimensionality as $\mathbb{C}$-vector spaces, it suffices to show $\underline{\rho}$ injective.

Let $\theta \in \ker\left(\underline{\rho}\right)$. Then, $\rho_j(\theta) = 0$ for each $j = 1, \ldots, t$, i.e. θ acts as 0 on each of the irreducibles $V_1, \ldots, V_t$. Applying Maschke's, it follows that θ must act as zero on every representation, in particular on $\mathbb{C}[G]$. Then, for every $\sum \beta_g g \in \mathbb{C}[G]$, $\theta \cdot \left(\sum \beta_g g\right) = 0$ so in particular $\theta \cdot 1 = 0$ hence $\theta = 0$ in $\mathbb{C}[G]$. Thus, $\underline{\rho}$ has trivial kernel as we wanted to show and thus $\mathbb{C}[G]$ and $\text{End}_{\mathbb{C}}(V_1) \oplus \cdots \oplus \text{End}_{\mathbb{C}}(V_t)$ are isomorphic as rings (moreover, as $\mathbb{C}$-algebras).

We look now at the centers of the two rings, since they are (in general) noncommutative. Namely,

$$Z(\mathbb{C}[G]) = \left\{\sum \lambda_g g \mid \left(\sum \lambda_g g\right)\theta = \theta\left(\sum \lambda_g g\right)\ \forall\, \theta \in \mathbb{C}[G]\right\}.$$

Since multiplication in $\mathbb{C}$ is commutative and "factors through" internal multiplication, it follows that $\sum \lambda_g g \in Z(\mathbb{C}[G])$ iff it commutes with every group element, i.e.

$$\Big(\sum \lambda_g g\Big)h = h\Big(\sum \lambda_g g\Big) \Leftrightarrow \sum_g \Big(\lambda_g h^{-1}gh\Big) = \sum_g \lambda_g g$$
$$\Leftrightarrow \sum_g \lambda_{h^{-1}gh} g = \sum_g \lambda_g g$$
$$\Leftrightarrow \lambda_{h^{-1}gh} = \lambda_g \ \forall\, g \in G.$$

Hence, $\sum \lambda_g g \in Z(\mathbb{C}[G])$ iff $\lambda_{h^{-1}gh} = \lambda_g$ for every $g, h \in G$. It follows, then, that the induced map $g \mapsto \lambda_g$ a class function, and thus $\dim_{\mathbb{C}}(Z(\mathbb{C}[G])) = h(G)$.

On the other hand, $\dim_{\mathbb{C}}\Big(Z\Big(\mathrm{End}_{\mathbb{C}}\Big(V_j\Big)\Big)\Big) = 1$ (by representing as matrices, for instance, one can see that only scalar matrices will commute with all other matrices), hence $\dim_{\mathbb{C}}(Z(\mathrm{End}_{\mathbb{C}}(V_1) \oplus \cdots \oplus \mathrm{End}_{\mathbb{C}}(V_t))) = t$. $\underline{\rho}$ naturally restricts to an isomorphism of these centers, hence we conclude justly $t = h(G)$. ■

Remark 1.4: By picking bases for each irreducible representation $V_1, \ldots, V_t$, we can realize more concretely that

$$\mathbb{C}[G] \simeq M_{d_1}(\mathbb{C}) \oplus \cdots \oplus M_{d_t}(\mathbb{C}),$$

where $d_j := \dim\Big(V_j\Big)$; in short, then, $\mathbb{C}[G]$ completely determined, as a group-ring, by

- the number of conjugacy classes in G, t; and
- the dimension of each irreducible representation, $d_1, \ldots, d_t$.

In particular, then, there may exist two non-isomorphic groups with isomorphic group rings.

§1.4 Fourier Analysis on Finite Abelian Groups

↪**Definition 1.8**: For a finite group G, let

$$L^2(G) = \{\text{square integrable functions } G \to \mathbb{C}\},$$

equipped with the L^2-norm, $\|f\|^2 = \frac{1}{\#G}\sum_{g\in G}|f(g)|^2$. This is a vector space isomorphic to $\mathbb{C}^{\#G}$. We make the space a Hilbert space by defining

$$\langle f_1, f_2\rangle = \frac{1}{\#G}\sum_{g\in G}\overline{f_1(g)}f_2(g).$$

↪**Definition 1.9**: Denote by $\hat{G} = \{\chi_1, \ldots, \chi_N\}$ the set of irreducible characters of G. Then, $\hat{G}$ an orthonormal family of functions in $L^2(G)$.

We suppose for now G abelian. In this case, $\#\hat{G} = \#G$ so $\hat{G}$ is an orthonormal basis for $L^2(G)$ (comparing dimensions). In particular, one can prove that $\hat{G}$ is abstractly isomorphic to G as a group.

↪**Definition 1.10**: Given $f \in L^2(G)$, the function $\hat{f} : \hat{G} \to \mathbb{C}$ is defined by

$$\hat{f}(\chi) = \frac{1}{\#G} \sum_{g \in G} \overline{\chi}(g) f(g),$$

called the *Fourier transform* of f over G. Then,

$$f = \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi,$$

is called the *Fourier inversion formula*.

⊛ **Example 1.2**: Consider $G = \mathbb{R}/\mathbb{Z}$. $L^2(G)$ space of $\mathbb{C}$-valued periodic functions on $\mathbb{R}$ which are square integrable on $[0,1]$. Then, $\hat{G}$ abstractly isomorphic to $\mathbb{Z}$. Write $\hat{G} = \{\chi_n \mid n \in \mathbb{Z}\}$. Then, remark that

$$\chi_n : \mathbb{R}/\mathbb{Z} \to \mathbb{C}^\times, \qquad \chi_n(x) = e^{2\pi i n x}$$

gives the characteristic function for any integer n. More precisely, its not hard to see that the map $\mathbb{R} \to \mathbb{C}^\times, x \mapsto e^{2\pi i n x}$ factors through (is constant on integer multiples) $\mathbb{Z}$.

To speak about orthogonality of members of $\hat{G}$, we must define a norm. We can identity $\mathbb{R}/\mathbb{Z}$ with $[0,1]$, and so write

$$\langle f_1, f_2 \rangle := \int_0^1 \overline{f_1(x)} f_2(x)\, \mathrm{d}x.$$

Then, its not hard to see

$$\langle \chi_n, \chi_m \rangle = \int_0^1 e^{-2\pi i (m-n)x}\, \mathrm{d}x = \delta_m^n.$$

⊛ **Example 1.3**: Let $G = \mathbb{Z}/N\mathbb{Z}$ under addition. Note that G then a subgroup of $\mathbb{R}/\mathbb{Z}$, and in particular,

$$\hat{G} = \{\chi_0, \chi_1, \ldots, \chi_{N-1}\}, \qquad \chi_j(k) := e^{2\pi i j k/N}.$$

Then, one notices

$$\chi_{j_1} \cdot \chi_{j_2} = \chi_{j_1 + j_2},$$

so there is indeed a natural group structure on $\hat{G}$. Then, the Fourier transform in this case gives, for $f \in L^2(\mathbb{Z}/N\mathbb{Z})$,

$$\hat{f}(n) = \frac{1}{N} \sum_{k=0}^{N-1} e^{-2\pi i n k/N} f(k).$$

1.4.1 Application to Computing Particular Infinite Series

We consider an application of the theory we've developed on $G = \mathbb{Z}/N\mathbb{Z}$ to study particular infinite summations. Its well know that the harmonic series $1 + \frac{1}{2} + \frac{1}{3} + \cdots$ diverges. A natural extension is to study modified such series, for instance $1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots$ and to ask if this series converges, and if it does, to what?

To approach this question, we more generally consider, for $f \in L^2(\mathbb{Z}/N\mathbb{Z})$ (i.e. a complex-valued N-periodic function defined on the integers), the series

$$S(f) := \sum_{n=1}^{\infty} \frac{f(n)}{n},$$

when the summation exists. Remark then that $f \mapsto S(f)$ is linear. So, it suffices to consider the value of $S(f)$ on a basis of $L^2(\mathbb{Z}/N\mathbb{Z})$, which we've derived in the previous example, namely $\hat{G} = \left\{\chi_j : j = 0, ..., N-1\right\}$. We can explicitly compute $S\left(\chi_j\right)$:

$$\begin{aligned} S\left(\chi_j\right) &= \sum_{n=1}^{\infty} \frac{\chi_j(n)}{n} \\ &= \sum_{n=1}^{\infty} \frac{x^n}{n}, \qquad x := e^{\frac{2\pi i j}{N}} \\ &= -\log(1-x), \end{aligned}$$

where the final sequence converges on the unit circle in the complex plane centered at the $1 + 0i$.

In particular, if $j = 0$, $S(\chi_0)$ diverges. Otherwise, each χ_j maps onto the roots of unity hence the convergence is well-defined. In particular, then, we find

$$S\left(\chi_j\right) = \begin{cases} -\log\left(1 - e^{2\pi i \frac{j}{N}}\right) & \text{if } j \neq 0 \\ 0 & \text{else} \end{cases}.$$

Now, for a general function $f \in L^2(\mathbb{Z}/N\mathbb{Z})$, we find by the Fourier inversion formula

$$S(f) = S\left(\hat{f}(0)\chi_0 + \cdots + \hat{f}(N-1)\chi_{N-1}\right),$$

which certainly diverges if $\hat{f}(0) \neq 0$. Otherwise, we find by linearity

$$S(f) = \sum_{j=1}^{N-1} \hat{f}(j)(-\log(1-x)).$$

So, returning to our original example, we can define $f \in L^2(\mathbb{Z}/4\mathbb{Z})$ by $f(n) = \begin{cases} 0 & \text{if } n \text{ even} \\ 1 & \text{if } n{=}1{+}4k \\ -1 & \text{if } n{=}3{+}4k \end{cases}$. Then, we find

$$1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{9}-\cdots = S(f)$$
$$= \frac{1}{2i}(S(\chi_1) - S(\chi_3))$$
$$= \frac{1}{2i}(-\log(1-i)+\log(1+i))$$
$$= \frac{1}{2i}\left(-\log\left(\sqrt{2}\right)+\frac{\pi i}{4}+\log\left(\sqrt{2}\right)+\frac{\pi i}{4}\right) = \frac{\pi}{4}.$$

§1.5 Fourier Analysis on Non-Abelian Finite Groups

When G abelian, recall that $\mathbb{C}[G]$ was a commutative ring isomorphic to $\bigoplus_{\chi\in\hat{G}}\mathbb{C}$. More generally, we find an isomorphism

$$\Phi : \mathbb{C}[G] \to \oplus_{j=1}^{h} \operatorname{End}_{\mathbb{C}}\left(V_j\right) \simeq \oplus_{j=1}^{h} M_{d_j\times d_j}(\mathbb{C}),$$

where $h = h(G)$, V_j enumerate the irreducible representations of G, and $d_j := \dim_{\mathbb{C}}\left(V_j\right)$.

↪**Definition 1.11** (Fourier Transform): Given a function $f : G \to \mathbb{C}$, denote by

$$\theta_f = \sum_{g\in G} f(g)g$$

its corresponding element in $\mathbb{C}[G]$. Then, its corresponding image under Φ in $\bigoplus \operatorname{End}\left(V_j\right)$ is called the *Fourier transform* of f, i.e.

$$\hat{f} = (T_1, ..., T_h) \in \bigoplus \operatorname{End}\left(V_j\right),$$

a h-tuple of matrices where T_i a $d_i \times d_i$matrix.

1.5.1 Random Products in Groups

↪**Definition 1.12** (Probability Measure on a Group): A probability measure on a group G is a function $\mu : G \to [0,\infty)$ such that $\sum_g \mu(g) = 1$. Then, we can view μ as living naturally both in $\mathbb{R}^G$ and $\mathbb{R}[G]$ through the standard identification.

One of the key properties we notice by viewing μ as living in $\mathbb{R}[G]$ is in multiplication; multiplication in $\mathbb{R}[G]$ corresponds to convolution of functions. Namely, if μ_1, μ_2 two measures on G, then

$$(\mu_1 \circledast \mu_2)(g) = \sum_{\substack{(g_1,g_2)\in G\times G,\\ g_1g_2=g}} \mu_1(g_1)\mu_2(g_2) = \mu_1 \times_{\mathbb{R}[G]} \mu_2$$
$$= \mathbb{P}(\text{getting } g \text{ from a random product of } g_1, g_2 \text{ with } g_i \text{ picked according to } \mu_i).$$

For a fixed probability measure μ, then, we wish to investigate the limiting behavior of $\mu^{\circledast N}$ (μ convolved with itself N times for large N), which corresponds to the likelihood of obtaining a particular element from large numbers of products in the group.

↪**Definition 1.13**: Define the support

$$\operatorname{supp}(\mu) = \{g \in G \mid \mu(g) \neq 0\},$$

and the 2 subgroups

$$G_\mu := \text{subgroup generated by } g \in \operatorname{supp}(\mu),$$

$$G_\mu^+ := \text{subgroup generated by } \{g^{-1}h \mid g, h \in \operatorname{supp}(\mu)\}.$$

Notice then $G_\mu^+ \subset G_\mu \subset G$.

↪**Theorem 1.11**: Let μ a probability measure on G. Then, if $G_\mu^+ = G$, then $\lim_{N\to\infty} \mu^{\circledast N} = \mu_{\text{unif}}$, where μ_{unif} the uniform probability distribution which assigns $\frac{1}{\#G}$ to each element in G.

§1.6 Character Tables of S_4, A_5 and $\mathrm{GL}_3(\mathbb{F}_2)$

1.6.1 S_4

For S_4, we denote the conjugacy classes by $1A, 2A, 2B, 3A, 3B, 4A$ as the conjugacy classes of elements of the form $(), (12)(34), (12), (123), (1234)$ respectively.

	$1A$	$2A$	$2B$	$3A$	$4A$
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	2	2	0	-1	0
χ_4	3	-1	1	0	-1
χ_5	3	-1	-1	0	1

χ_1 is the trivial representation. χ_2 is the sign representation given by $\sigma \mapsto \operatorname{sgn}(\sigma) \in \{-1, 1\} \subseteq \mathbb{C}^x$. χ_3 comes from noticing that $K_4 = \mathbb{Z}/2 \times \mathbb{Z}/2 = 1A \sqcup 2A \subseteq S_4$ gives $S_4/K_4 \simeq S_3$. We then can find a new representation by composing the quotient map $\pi : S_4 \to S_3$ with a representation $\rho : S_3 \to \operatorname{Aut}_{\mathbb{C}}(V)$. Remember that there are three irreducible representations of S_3. The first two are the trivial and sign, already accounted for here. The last is the unique two-dimensional representation where $\chi(2A) = 0$ and $\chi(3A) = -1$ (these are the conjugacy classes in S_3 now). Under the quotient map, then, we find that

- since $1A, 2A$ contained in K_4, they are mapped to the identity in $\operatorname{Aut}(\mathbb{C}^2)$ so have trace 2;
- $2B, 4A$ must be mapped to elements of order 2 in S_3 (i.e. in $2A$) under π and thus must have trace 0;
- $3A$ must map to elements of order 3 in S_3 under π so must have trace -1.

This characterizes χ_3.

χ_4 comes from the standard representation on a 4 dimensional vector space (by permuting basis vectors), then subtracting off the trivial representation. This results in a character where each entry equals the number of fixed points each conjugacy class has, minus 1.

χ_5 comes from considering the homomorphism representation found from $V_5 = \mathrm{Hom}(V_2, V_4)$, where V_2, V_4 the vector spaces upon which χ_2, χ_4 "act". Hence, V_5 is a three dimensional representation, with $\chi_5 = \overline{\chi}_2\chi_4$.

1.6.2 A_5

For A_5, denote the conjugacy classes $1A, 2A, 3A, 5A, 5B$.

	$1A$	$2A$	$3A$	$5A$	$5B$
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	5	1	-1	0	0
χ_4	3	-1	0	$1+\zeta+\zeta^{-1}$	$1+\zeta^2+\zeta^{-2}$
χ_5	3	-1	0	$1+\zeta^2+\zeta^{-2}$	$1+\zeta+\zeta^{-1}$

χ_1 trivial. χ_2 comes from the standard representation, minus the trivial. χ_3 similarly comes from the action of A_5 on the coset space S_5/F_{20}, or equivalently on A_5/D_{10}, minus the trivial again.

For the last two, we can check by dimensionality that it must be that the dimensions of both must be 3, so we are looking for representations $\rho : A_5 \to \mathrm{Aut}_{\mathbb{C}}(\mathbb{C}^3)$. Let $g \in 5A$. Notice then that g must have at most three eigenvalues, which are fifth roots of unity. But also, notice that g and g^{-1} are conjugate in A_5, and namely $g, g^{-1} \in 5A$. Hence, since a linear transformation has inverse eigenvalues of its inverse, it follows that the set of eigenvalues for g must be closed under taking inverses. So, the eigenvalues must be of the form $\{1, \zeta, \zeta^{-1}\}$ or $\{1, \zeta^2, \zeta^{-2}\}$ where ζ a primitive root of unity. It follows then that either $\mathrm{tr}(5A) = 1+\zeta+\zeta^{-1}$ or $1+\zeta^2+\zeta^{-2}$, with, by symmetrical argument, gives the trace of $5B$ since $g \in 5A \Rightarrow g^2 \in 5B$.

Then, to find $\chi(3A) =: x_3$, taking the inner product with χ_2 we find

$$\begin{aligned} 0 &= 12 + 20x_3 - 12\left(1+\zeta+\zeta^{-1}\right) - 12\left(1+\zeta^2+\zeta^{-2}\right) \\ &= 20x_3 - 12\left(\underbrace{1+\zeta+\zeta^2+\zeta^3+\zeta^4}_{=0}\right) \Rightarrow x_3 = 0. \end{aligned}$$

From here, one can compute $\chi(2A)$ using orthogonality relations.

1.6.3 $\mathrm{GL}_3(\mathbb{F}_2)$

size:	1	21	56	42	24	24
	$1A$	$2A$	$3A$	$4A$	$7A$	$7B$
χ_1	1	1	1	1	1	1
χ_2	6	2	0	0	-1	-1
χ_3	7	-1	1	-1	0	0

χ_1 trivial. We consider χ_V given by G acting on $\mathbb{F}_2^3$ in the standard way (as three by three matrices) Then, the character is just given by the number of fixed points each element has, so in this case the number of fixed nonzero vectors.

- $1A$ 7, being the dimension

- A typical element of $2A$ looks like $\begin{pmatrix} 1 & & 1 \\ & 1 & \\ & & 1 \end{pmatrix}$ which has trace 3.
- $g \in 3A$ has minimal polynomial $(x-1)\left(x^2+x+1\right)$ so has a one-dimensional eigenspace so fixes one nonzero vector.
- $g \in 4A$ has minimal polynomial $(x-1)^3$ so by similar reasoning as $3A$ fixes a one-dimensional eigenspace.
- $g \in 7A$ or $7B$ must cyclically permute the basis vectors so fixes none so has trace 0.

In summary:

	$1A$	$2A$	$3A$	$4A$	$7A$	$7B$
χ_V	7	3	1	1	0	0

This is not irreducible by checking orthogonality relations, but we obtain χ_2 by subtracting off χ_1.

For χ_3, consider $X = \{\text{sylow} - 7 \text{ subgroups}\}$. One can check $\#X = 8$, and we have a natural action of G on X by conjugation, which is isomorphic to the action of G on $G/N(\text{Sylow} - 7)$ so $H := N(\text{Sylow} - 7)$ has cardinality 21. Then, the trace of each element is just the number of fixed cosets each element has acting on G/H. We then subtract off 1 from this number to obtain χ_3.

- $g \in 1A$ must have trace 8 so $\chi_3(1A) = 7$
- if $g \in 2A$, $gaH = aH \Leftrightarrow a^{-1}ga \in H$, but g of order 2 and thus so is $a^{-1}ga$, but H a group of cardinality of order 21 so such an element can't live in it.Thus g has no fixed points and $\chi_3(2A) = -1$. In particular g as a permutation looks like 4 disjoint 2 cycles.
- if $g \in 4A$, similar reasoning follows and we find $\chi_3(4A) = -1$ and g looks like 2 disjoint 4 cycles.
- $g \in 7A, 7B$ must act as a 7-cycle and so has one fixed point and thus $\chi_3(7A) = \chi_3(7B) = 0$.
- we can compute $\chi_3(3A)$ by checking the orthogonality relations by taking the inner product of it with itself. Computing this we find that $\chi_3(3A) = \pm 1$. We conclude it must be 1 by remarking that $3A$ acts on G/H either by a single 3 cycles (hence with 5 fixed points) or two three cycles (hence with 2), so it must be that the second case holds which gives us a character of 1.

§1.7 Induced Representations

Let G a finite group and $H \subseteq G$, and take $\chi \in \text{Hom}(H, \mathbb{C}^\times)$ a one-dimensional representation of H. Consider the space

$$V_\chi = \{f : G \to \mathbb{C} \mid f(xh) = \chi(h) \cdot f(x) \ \forall\, h \in H\}.$$

Then,

↪**Proposition 1.10**:
1. G acts (linearly) on V_χ by the rule $gf(x) = f\left(g^{-1}x\right), \forall\, x \in G$.
2. $\dim\left(V_\chi\right) = [G : H]$

Proof.

1. We need to show $gf \in V_\chi$. We compute,
$$gf(xh) = f\left(g^{-1}(xh)\right) = f\left(\left(g^{-1}x\right)h\right) = \chi(h)f\left(g^{-1}x\right) = \chi(h)(gf)(x),$$
for any $x \in G, h \in H, f \in V_\chi$, as required.
2. Let $a_1, ..., a_t$ be a set of coset representatives for H, i.e. $G = a_1H \sqcup \cdots \sqcup a_tH$. Then, we claim that the map $f \mapsto (f(a_1), ..., f(a_t))$, $V_\chi \to \mathbb{C}^t$ a $\mathbb{C}$-vector space isomorphism.

Injective: If f in the kernel of this map, then $f(a_1) = \cdots = f(a_t) = 0$. But $f \in V_\chi$ so $f\left(a_jh\right) = \chi(h)f\left(a_j\right) = 0$ for any $h \in H$, $j = 1, ..., t$. Any element in G is in some a_jH so equals a_jh for some $h \in H$, so we conclude that f must be identically 0 and so this map injective.

Surjective: Given $(\lambda_1, ..., \lambda_t) \in \mathbb{C}^t$, define f by $f\left(a_j\right) := \lambda_j$ for each j, and "extend" naturally to behave under action of H, namely $f\left(a_jh\right) := \chi(h)f\left(a_j\right) = \chi_h\lambda_j$. ■

The representation V_χ is called the *induced* representation of χ from H to G. We sometimes write
$$V_\chi = \mathrm{Ind}_H^G\chi.$$

If H is a quotient of G, then any representation of H gives a representation of G (we've done this many times before, such as with S_4 and S_3). But in general, these aren't easy to come by. But if H just a subgroup of G, which are far more common, then we can use the induced representation technique above to look at representations of G.

Let $\psi : H \to \mathbb{C}^\times$ some one-dimensional representation of H and $V_\psi = \mathrm{Ind}_H^G\psi$. We wish to find the induced character χ_{V_ψ}.

We begin by looking for a basis for V_ψ. For any $a \in G$, define $f_a \in V_\psi$ defined by
$$f_a : G \to \mathbb{C}, \qquad f_a(g) := \begin{cases} \psi(h) \text{ if } g = ah \in aH \\ 0 \quad\ \text{if } g \notin aH \end{cases}.$$

Then, if $a_1, ..., a_t$ coset representatives for H in G, $\beta := \left\{f_{a_1}, ..., f_{a_t}\right\}$ a basis for V_ψ.

Now, given $g \in G$, what is the matrix of g acting on V_ψ with respect to the basis β? We have that
$$g \cdot f_{a_j}(x) = f_{a_j}\left(g^{-1}x\right) = f_{ga_j}(x),$$
since, more precisely
$$gf_{a_j}(a_i) = \begin{cases} 0 \text{ if } g^{-1}a_i \notin a_jH \\ \psi(h) \text{ if } g^{-1} = a_jh' \end{cases}$$
and we can extend to general $g \in G$. Hence, if $a_1, ..., a_t$ are coset representatives, $ga_jH = a_iH$ for each a_j and some a_i, i.e. g permutes the coset representatives, modulo H. Hence, $ga_j = a_ih_{ij}$ for some $h_{ij} \in H$. So,
$$gf_{a_j} = f_{a_ih_{ij}} = \psi\left(h_{ij}\right)f_{a_i}.$$

Write $ga_iH = a_{i'}H$ so $ga_i = a_{i'}h_i$. With this, $gf_{a_1} = \psi(h_1)f_{a_1'}$, etc, and so in each ith column of our matrix there is a single nonzero entry in the i'th row with entry $\psi(h_i)$.

Thus,

$$\chi_{V_\psi}(g) = \sum_{\substack{i \mid ga_i = a_i h_i, \\ h_i \in H}} \psi(h_i) = \sum_{i=1}^{t} \tilde{\psi}\left(a_i^{-1} g a_i\right),$$

namely, we only sum over the h_i's that land the in the diagonal, which are only those that come from g fixing the respective cosets. We put $\tilde{\psi}$ to be ψ on H and 0 elsewhere. In all, them, we have proven the following theorem.

↪**Theorem 1.12**: Let $H \subseteq G$ and $\psi : H \to \mathbb{C}^\times$ a one-dimensional representation of H. Then, the induced character from H to G is given by

$$\chi_{\mathrm{Ind}_H^G \psi}(g) = \sum_{\substack{aH \in G/H, \\ \text{s.t.} a^{-1}ga \in H}} \psi(a^{-1}ga) = \sum_{a \in G/H} \tilde{\psi}(a^{-1}ga),$$

where

$$\tilde{\psi}(g) = \begin{cases} 0 & \text{if } g \notin H \\ \psi(h) & \text{if } g \in H \end{cases}.$$

Let's massage.

↪**Theorem 1.13**:

$$\chi_{V_\psi}(g) = \chi_{\mathrm{Ind}_H^G \psi}(g) = \frac{\#G}{\#H} \cdot \frac{1}{\#C(g)} \sum_{\gamma \in C(g) \cap H} \psi(\gamma),$$

where $C(g)$ the conjugacy class of the element g,

Proof.

$$\begin{aligned}
\chi_{V_\psi}(g) &= \sum_{\substack{aH \in G/H, \\ \text{s.t.} a^{-1}ga \in H}} \psi(a^{-1}ga) \\
&= \frac{1}{\#H} \sum_{\substack{a \in G, \\ \text{s.t.} a^{-1}ga \in H}} \psi(a^{-1}ga) \\
&= \frac{\#Z(g)}{\#H} \sum_{\substack{a \in Z(g)/G, \\ \text{s.t } a^{-1}ga \in H}} \psi(a^{-1}ga) \\
&= \frac{\#G}{\#H} \frac{1}{\#C(g)} \sum_{\gamma \in C(g) \cap H} \psi(\gamma),
\end{aligned}$$

where $Z(g) = \{b \in G \mid bg = gb\}$ the centralizer of G, where $\#Z(g) = \frac{\#G}{\#C(g)}$ by the orbit-stabilizer theorem (from G acting on $C(g)$ by conjugation). ■

1.7.1 Back to $\mathrm{GL}_3(\mathbb{F}_2)$

Let $H \subseteq G = \mathrm{GL}_3(\mathbb{F}_2)$ the normalizer of a Sylow-7 subgroup; then $\#H = 21$ (8 Sylow-7 subgroups, $\frac{168}{8} = 21$). Let

$$\psi : H \to \mathbb{C}^x$$

and

$$V = \mathrm{Ind}_H^G \psi$$

the induced character. Then, we know $\dim(V) = 168/21 = 8$. Let P_7 be some Sylow-7 subgroup. Then, we find that

$$H/P_7 \simeq \mathbb{Z}/3\mathbb{Z},$$

so our representation factors to

$$H \twoheadrightarrow \mathbb{Z}/3\mathbb{Z} \to \mathbb{C}^\times,$$
$$1 \mapsto e^{2\pi i/3}.$$

So specializing our formula we found in the previous section, we know

$$\chi_{V_\psi}(g) = \frac{8}{\#C(g)} \sum_{\gamma \in H \cap C(g)} \psi(\gamma).$$

We compute for g in distinct conjugacy classes:

#	C	χ_{V_ψ}
1	$1A$	8
21	$2A$	0
56	$3A$	-1
42	$4A$	0
24	$7A$	1
24	$7B$	1

- The case for $1A$ is simple.
- The case for $2A$ and $4A$ are trivial since for $C = 2A, 4A$, $C \cap H = \varnothing$, since H a group of odd cardinality, and C consists only of elements of even order, hence they must have empty intersection, so the summation in the character formula is over nothing.
- For $3A$, we need to compute $3A \cap H$. We know that

  $$\varphi : H \twoheadrightarrow \mathbb{Z}/3\mathbb{Z},$$

  so it must be that

  $$P_7 \mapsto 0, \qquad 7 \text{ elts of order } 3 \mapsto 1, \qquad 7 \text{ elts of order } 3 \mapsto 2,$$

so

$$3A \cap H = \varphi^{-1}(1) \sqcup \varphi^{-1}(2).$$

Hence,

$$\begin{aligned}\chi_{V_\psi}(3A) &= \frac{1}{7}\left(\sum_{g\in\varphi^{-1}(1)} \psi(g) + \sum_{g\in\varphi^{-1}(2)} \psi(g)\right) \\ &= \frac{1}{7}\left[7e^{2\pi i/3} + 7e^{4\pi i/3}\right] \\ &= e^{2\pi i/3} + e^{4\pi i/3} = -1.\end{aligned}$$

- For $g \in 7A$,

$$\chi_{V_\psi}(g) = \frac{8}{24}\sum_{g\in 7A\cap H} \psi(g).$$

Its easy to see $\psi(g) = 1$, since g of order 7. So, the difficulty lies in computing the size $7A \cap H$. There are certainly 6 elements of order 7 in H, but which are in 7A versus 7B? The key fact to notice is that, if $g \in 7A, g^2, g^4 \in 7A$ as well, and $g^{-1} = g^6$, g^3 and g^5 are in $7B$, which one verifies by checking the minimal polynomials of the two sets of elements (either $x^3 + x + 1, x^3 + x^2 + 1$). Thus,

$$\chi_{V_\psi}(g) = \frac{1}{3}(1 + 1 + 1) = 1,$$

for both $g \in 7A, 7B$.

One can take the inner product $\langle \chi_{V_\psi}, \chi_{V_\psi} \rangle$ and find that it is equal to 1, hence this new representation is irreducible. Naming this representation χ_4, we find the character table so far to be (from the previous section):

size:	1	21	56	42	24	24
	$1A$	$2A$	$3A$	$4A$	$7A$	$7B$
χ_1	1	1	1	1	1	1
χ_2	6	2	0	0	-1	-1
χ_3	7	-1	1	-1	0	0
χ_4	8	0	-1	0	1	1
χ_5	d_5	?	?	?	?	?
χ_6	d_6	?	?	?	?	?

We know then from the general theory that we are missing two representations. We know that the sum of the squares of the dimensions should equal the cardinality of the group, so

$$168 = 1 + 36 + 49 + 64 + d_5^2 + d_6^2 \Rightarrow d_5^2 + d_6^2 = 18.$$

It's not hard to see the only way this is possible is that $d_5 = 3, d_6 = 3$.

§1.8 Tensor Products

We are often interested in generating new representations from exists ones. Suppose V_1, V_2 are two representations.

- *Direct sum:*
$$V_1 \oplus V_2,$$
with character $\chi_{V_1 \oplus V_2} = \chi_{V_1} + \chi_{V_2}$.
- *Hom* representation: given by G acting on
$$\mathrm{Hom}_{\mathbb{C}}(V_1, V_2),$$
given by
$$g * T = g \circ T \circ g^{-1}, \qquad g \in G, T \in \mathrm{Hom}_{\mathbb{C}}(V_1, V_2),$$
which had character $\chi_{\mathrm{Hom}_{\mathbb{C}}(V_1,V_2)} = \overline{\chi_{V_1}} \cdot \chi_{V_2}$.
- *Dual* representation: given by the action on $V_1^* := \mathrm{Hom}(V_1, \mathbb{C})$ defined by $g\ell = \ell \circ g^{-1}$. This gives $\chi_{V_1^*} = \overline{\chi_{V_1}}$

We define now the *tensor representation*:

↪**Definition 1.14** (Tensor Product): Given representations V_1, V_2, put
$$V_1 \otimes V_2 = \mathrm{Hom}_{\mathbb{C}}(V_1^*, V_2).$$

Then, one readily verifies $\dim(V_1 \otimes V_2) = \dim(V_1) \cdot \dim(V_2)$.

More concretely, let $v_1 \in V_1$ and $v_2 \in V_2$. Then for $\ell \in V_1^*$, we can define
$$v_1 \otimes v_2(\ell) := \ell(v_1) \cdot v_2 \in V_2.$$
One readily verifies that this definition genuinely defines an element of $\mathrm{Hom}_{\mathbb{C}}(V_1^*, V_2)$.

One notices too that $\otimes$ is *bilinear* in both arguments, namely for any $v_1, v_1' \in V_1$, $v_2, v_2' \in V_2$, $\lambda \in \mathbb{C}$ and $\ell \in V_1^*$, then
$$(\lambda v_1 + v_1') \otimes v_2 = \lambda(v_1 \otimes v_2) + (v_1' \otimes v_2),$$
and also
$$v_1 \otimes (\lambda v_2 + v_2') = \lambda(v_1 \otimes v_2) + (v_1 \otimes v_2').$$
Let $e_1, \ldots, e_n$ a basis for V_1 and $f_1, \ldots, f_m$ a basis for V_2, and consider $v_1 = a_1 e_1 + \cdots + a_n e_n$, $v_2 = b_1 f_1 + \cdots + b_m f_m$ for $a_i, b_j \in \mathbb{C}$. Then, using the bilinearity, we find
$$\begin{aligned} v_1 \otimes v_2 &= (a_1 e_1 + \cdots + a_n e_n) \otimes (b_1 f_1 + \cdots + b_m f_m) \\ &= \sum a_i b_j \big(e_i \otimes f_j\big), \end{aligned}$$
so we find from this that the elements $e_i \otimes f_j$ for $1 \le i \le n, 1 \le j \le m$ span $V_1 \otimes V_2$ and hence define a basis.

Now, G acts on $V_1 \otimes V_2$ by the rule

$$g \cdot (v_1 \otimes v_2) = (gv_1) \otimes (gv_2).$$

Hence, we find

$$\chi_{V_1 \otimes V_2} = \chi_{\mathrm{Hom}\,(V_1^*, V_2)} = \overline{\chi_{V_1^*}} \cdot \chi_{V_2} = \chi_{V_1} \cdot \chi_{V_2},$$

using the character properties above.

We can also prove this directly. Let $g \in G$ and let $e_1, \ldots, e_n$ be a basis for V_1 of eigenvectors for g, and $f_1, \ldots, f_m$ a basis for V_2 of eigenvectors for g. Suppose $g \cdot e_i = \lambda_i e_i$, $g \cdot f_j = \mu_j f_j$, for some $\lambda_i, \mu_j \in \mathbb{C}$. Then,

$$g \cdot \big(e_i \otimes f_j\big) = (g \cdot e_i) \otimes \big(g \cdot f_j\big) = \big(\lambda_i e_i \otimes \mu_j f_j\big) = \big(\lambda_i \mu_j\big)\big(e_i \otimes f_j\big).$$

Hence, we find

$$\mathrm{tr}\big(\rho_{V_1 \otimes V_2}\big)(g) = \sum_{\substack{i=1,\ldots,n \\ j=1,\ldots,m}} \lambda_i \mu_j = \sum_{i=1}^{n} \lambda_i \sum_{j=1}^{m} \mu_j = \chi_{V_1}(g) \cdot \chi_{V_2}(g).$$

⊛ **Example 1.4** (A_5): Recall the character table of A_5,

	1	15	20	12	12
	$1A$	$2A$	$3A$	$5A$	$5B$
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	5	1	-1	0	0
χ_4	3	-1	0	$1+\zeta+\zeta^{-1}$	$1+\zeta^2+\zeta^{-2}$
χ_5	3	-1	0	$1+\zeta^2+\zeta^{-2}$	$1+\zeta+\zeta^{-1}$

We consider various tensors of representations:

	$1A$	$2A$	$3A$	$5A$	$5B$
$V_2 \otimes V_3$	9	1	0	-1	-1

which we notice to equal the character of $\chi_4 \oplus \chi_5$; namely, $V_2 \otimes V_3 \simeq V_4 \oplus V_5$.

Also

	$1A$	$2A$	$3A$	$5A$	$5B$
$V_2 \otimes V_4$	12	0	0	$\frac{-1-\sqrt{5}}{2}$	$\frac{-1+\sqrt{5}}{2}$

from which we find

$$V_2 \otimes V_4 \simeq V_3 \oplus V_4 \oplus V_5.$$

§1.9 Cute Applications of Representation Theory

1.9.1 The Pillaging Knights

Suppose we are given N knights, whom, after a long night of pillaging, sit at a round table to share their spoils of war. Each knight decides to split his earnings equally among his two neighbors. What happens after many iterations?

The wealth distribution may be modelled as a function on $\mathbb{Z}/N\mathbb{Z}$; each knight is identified with some element of $\mathbb{Z}/N\mathbb{Z}$, and the wealth is given by $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$. Then,

$$f \in L^2(\mathbb{Z}/N\mathbb{Z}) = \bigoplus_{j=0}^{N-1} \mathbb{C} \cdot e^{2\pi ijx/N}.$$

Then, "wealth distribution" can be seen as a function $T : L^2 \to L^2$ given by

$$Tf(x) \coloneqq \frac{1}{2}(f(x-1) + f(x+1)).$$

Then,

$$\begin{aligned} Te^{2\pi ijx/N} &= \frac{1}{2}\left(e^{2\pi ij(x+1)/N} + e^{2\pi ij(x-1)/N}\right) \\ &= \frac{1}{2}\left(e^{2\pi ij/N} + e^{-2\pi ij/N}\right)e^{2\pi ijx/N} \\ &= \cos(2\pi j/N)e^{2\pi ijx/N}. \end{aligned}$$

Then, we may write $f = \hat{f}(0)f_0 + \hat{f}(1)f_1 + \cdots + \hat{f}(N-1)f_{N-1}$, so

$$Tf = \hat{f}(0)f_0 + \hat{f}(1)\cos\left(\frac{2\pi}{N}\right)f_1 + \cdots + \hat{f}(N-1)\cos\left(\frac{2\pi(N-1)}{N}\right)f_{N-1},$$

and hence

$$\widehat{Tf}(j) = \hat{f}(j)\cos\left(\frac{2\pi j}{N}\right).$$

Thus,

$$\widehat{T^M f}(j) = \hat{f}(j)\left(\cos\left(\frac{2\pi}{N}\right)\right)^M.$$

1.9.2 Functions on Mathematical Objects with Symmetry Groups

Let X a "mathematical object", G a group of symmetries and $V = L^2(X) = \mathbb{C}$-valued functions on X. We assume X finite (hence G finite and V finite). We are interested in studying operators $T : L^2(X) \to L^2(X)$.

Suppose X a set of vertices of a graph; define for $\varphi \in L^2(X)$, $(T\varphi)(x) = \sum_{(y,x) \text{ an edge}} \varphi(y)$; T the adjacent operator, extended to functions on $\mathbb{C}$. We claim T commutes with the action of G; write $y \sim x$ if the vertex y adjacent to the vertex x:

$$\begin{aligned} (T \circ g)(\varphi)(x) &= T(g\varphi)(x) \\ &= \sum_{y \sim x} (g\varphi)(y) \\ &= \sum_{y \sim x} \varphi(g^{-1}y), \end{aligned}$$

while on the other hand

$$\begin{aligned}(g \circ T)(\varphi)(x) &= g(T(\varphi))(x) \\ &= T(\varphi)\left(g^{-1}x\right) \\ &= \sum_{y \sim g^{-1}x} \varphi(y),\end{aligned}$$

which are equal upon change of index.

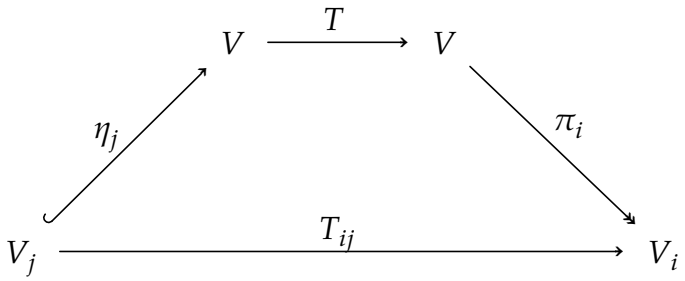
Suppose X the faces of a cube, and $V = L^2(X)$. Define

$$T\varphi(F) = \frac{1}{4} \sum_{F' \text{ adjacent to } F} \varphi(F').$$

What is the spectrum of T?

↪**Theorem 1.14**: If $V = V_1 \oplus \cdots \oplus V_t$, where the V_j's are distinct irreducible representations of G, then T maps V_j to itself, and in particular acts as a scalar on V_j.

Proof. T can be written as a $t \times t$ "matrix of matrices", $\left(T_{ij}\right)$, where $T_{ij} : V_j \to V_i$. Moreover, each $T_{ij} \in \mathrm{Hom}_G\left(V_j, V_i\right)$ (being G-equivariant). More specifically:



Where $\eta_j \in \mathrm{Hom}_G\left(V_j, V\right)$ the inclusion map, $\pi_i \in \mathrm{Hom}_G(V, V_i)$ the projection map (one readily verifies they are actually G-equivariant) and by construction $T \in \mathrm{Hom}_G(V, V)$; hence, $T_{ij} = \pi_i T \eta_j \in \mathrm{Hom}_G\left(V_j, V_i\right)$. By Schur's Lemma, then, $T_{ij} = \begin{cases} 0 & \text{if } i \neq j \\ \lambda_i & \text{if } i = j \end{cases}$.

So, if $v \in V_j$, $T(v) \in V_j$ since

$$\begin{aligned}T(v) &= \pi_1 T(v) + \pi_2 T(v) + \cdots + \pi_t T(v) \\ &= T_{1j}v + \cdots + T_{tj}v \\ &= T_{jj}v = \pi_j v.\end{aligned}$$

■

Remark 1.5: More generally whenever $T : V \to V$ is linear and $V = V_1 \oplus \cdots \oplus V_t$, then we may write

$$v = (v_1, ..., v_t)^t,$$

where $v_j \in V_j$ i.e. $v = v_1 + \cdots + v_t$. In this notation,

$$Tv = \begin{pmatrix} T_{11} & T_{12} & \cdots & T_{1t} \\ T_{21} & T_{21} & \vdots & T_{2t} \\ \vdots & & & \vdots \\ T_{t1} & T_{t2} & \cdots & T_{tt} \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_t \end{pmatrix},$$

where $T_{ij} \in \mathrm{Hom}\big(V_j, V_i\big)$.

1.9.3 Functions on a Cube

Let $X =$ set of faces of a cube, and $V = L^2(X)$ acted on by $G = S_4$, the symmetry group the cube. Let $T : V \to V$ be defined by

$$T(\psi)(x) = \frac{1}{4} \sum_{y \sim x} \varphi(y),$$

where $y \sim x$ means y, x are adjacent faces; the sum is over all faces adjacent to x. Notice that T is G-equivariant; moreover we can view it as a 4-way "sharing" of the value on adjacent faces, as in the knight example but now sitting on a cube rather than a circle.

We aim to decompose $L^2(X)$ into a sum of irreducible representations. We have the character table of S_4;

	1	6	3	8	6
	$1A$	$2A$	$2B$	$3A$	$4A$
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	2	-1	0
χ_4	3	1	-1	0	-1
χ_5	3	-1	-1	0	1
$L^2(X)$	6	0	2	0	2

If χ the character of $L^2(X)$ then $\chi = m_1\chi_1 + \cdots + m_5\chi_5$; we determine m_i by taking the inner product of χ with each of the irreducible characters; whence we may write

$$\begin{aligned} L^2(X) &= V_1 \oplus V_3 \oplus V_5 \\ &= \{\text{constant functions}\} \oplus L^2(X)_{+,0} \oplus L^2(X)_- \end{aligned}$$

We'll say a function $\varphi : X \to \mathbb{C}$ is *even* if $\varphi(x) = \varphi(x')$ where x' the face opposite of x. The space, call it $L^2(X)_+$, of even functions is naturally G-stable; if $\varphi \in L^2(X)_+$ and $g \in G$, then $g\varphi(x) = g\varphi(x')$ while also $\varphi\big(g^{-1}\big)x = g\varphi(x)$, $\varphi\big(g^{-1}x'\big) = g\varphi(x')$, hence we find $\varphi\big(g^{-1}x\big) = \varphi\big(g^{-1}x'\big)$, hence G sends even functions to even functions.

This space already contains constant function, so we want to consider the complementary space;

$$L^2(X)_{+,0} := \left\{ \varphi : X \to \mathbb{C} \mid \varphi \text{ even and } \sum_{x \in X} \varphi(x) = 0 \right\}.$$

Similarly, consider $L^2(X)_-$ =space of odd functions $= \{\varphi : X \to \mathbb{C} | \ \varphi(x') = -\varphi(x)\}$.

Our T above preserves V_1, V_3, V_5. Namely,

$$T(\mathbb{1}_X) = \mathbb{1}_X,$$

so 1 an eigenvalue with eigenvector "1". If $\varphi \in V_5$,

$$T(\varphi) = 0,$$

so 0 an eigenvalue with multiplicity 3. If $\varphi \in V_3$, suppose φ a, b, c on adjacent faces so $a + b + c = 0$; then

$$T(\varphi)(x) = \frac{1}{4}(a + a + c + c) = -\frac{1}{2}b = -\frac{1}{2}\varphi(x),$$

so

$$T\varphi = -\frac{1}{2}\varphi,$$

hence $-\frac{1}{2}$ an eigenvalue with multiplicity 2.

§2 Midterm Practice

↪**Proposition 2.1**: Let $G = D_8$ be the dihedral group of order 8. Write down the character table of G.

Proof. We can realize G as a subgroup of S_4 by identifying vertices of the square with numbers 1 through 4; this gives the following class equation for G:

$$\begin{aligned} G &= \{1\} \sqcup \{(13)(24)\} \sqcup \{(1234), (1432)\} \sqcup \{(12)(34), (14)(23)\} \sqcup \{(24), (13)\} \\ &=: (1) \sqcup \quad (2) \quad \sqcup \quad (3) \quad \sqcup \quad (4) \quad \sqcup \quad (5). \end{aligned}$$

Remark that $(1) \cup (2) \simeq \mathbb{Z}/2\mathbb{Z}$, and in particular is equal to the center of G. Hence, if we let ρ be a representation of G, we can "factor through" the center, and consider instead

$$\rho : G/(1) \cup (2) \to \mathrm{Aut}_{\mathbb{C}}(V).$$

One readily verifies that $G/(1) \cup (2) \simeq K_4$, which is an abelian group hence every such irreducible representation is one-dimensional, and in particular there are 4 of them. In each, $\chi((2)) = \chi((1)) = 1$, and χ is always just a second root of unity (namely either 1 or minus 1). In particular, we can choose $\chi((3))$ and $\chi((5))$ to be either 1 or minus 1, then $\chi((4))$ is must be equal to the product of these. This gives 4 total options;

	(1)	(2)	(3)	(4)	(5)

χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	-1	1
χ_4	1	1	-1	1	-1
χ_5	2	-2	0	0	0

The last row can either be computed via orthogonality relations, or by considering the action of D_8 described in Proposition 1.2. ■

↪**Proposition 2.2**: Let G be a finite group in which every element is conjugate to its inverse.
(a) Give an example of such a group.
(b) Show that the character of any complex representation of such a group is real-valued (all the entries of the character table are real).

Proof. (a) S_n, among others.

(b) We know $\chi(g^{-1}) = \overline{\chi(g)}$ (always). But if g conjugate to g^{-1}, since χ a class function, $\chi(g^{-1}) = \chi(g)$ so combining these two equalities we find $\chi(g) = \overline{\chi(g)}$, which is only possible if $\chi(g)$ real, namely has no imaginary part. ■

↪**Proposition 2.3**: Let G a finite group and $\rho : G \to \mathrm{GL}_n(\mathbb{R})$ a homomorphism. Show that for any integer $t \geq 1$, the matrix

$$M = \sum_{\mathrm{order}(g)=t} \rho(g)$$

is diagonalizable.

Proof. There exists a G-equivariant inner product $(\cdot,\cdot)$ on $\mathbb{R}^n$ (by replacing any arbitrary inner product with an averaging over the group). Then, for any $x, y \in \mathbb{R}^n$, we find

$$(Mx, y) = \sum_{\mathrm{ord}(g)=t} (\rho(g)x, y) = \sum_{\mathrm{ord}(g)=t} \left(x, \rho(g)^{-1} y\right) = \left(x, \sum_{\mathrm{ord}(g)=t} \rho(g^{-1})y\right),$$

but $\mathrm{ord}(g) = \mathrm{ord}(g^{-1})$, so we may change indices $g \to g^{-1}$ without changing the summation, and find

$$(Mx, y) = \left(x, \sum_{\mathrm{ord}(g)=t} \rho(g)y\right) = (x, My),$$

hence $M = M^*$, namely M self-adjoint. By the spectral theorem, it follows that M diagonalizable. ■

↪**Proposition 2.4**: Let χ be the character of a 2-dimensional representation of a finite group G, and assume that g is of order 4 for which $\chi(g) = 0$. Prove that $\chi(g^2)$ is either plus or minus 2.

Proof. Suppose $\rho(g) = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$, so $\chi(g) = 0$ as needed. Then,

$$\rho(g^2) = \begin{pmatrix} a^2 + bc & 0 \\ 0 & a^2 + bc \end{pmatrix},$$

so $\chi(g^2) = 2(a^2 + bc)$, while also g of order 4 so

$$I = \rho(g^4) = \begin{pmatrix} (a^2 + bc)^2 & 0 \\ 0 & (a^2 + bc)^2 \end{pmatrix},$$

hence $a^2 + bc = \pm 1$, and thus

$$\chi(g^2) = \pm 2.$$

■

↪**Proposition 2.5**: Let D_8 be the dihedral group of order 8 and Q the quaternion group. Show that the group rings $\mathbb{C}[D_8]$ and $\mathbb{C}[Q]$ are isomorphic, while the group rings $\mathbb{R}[D_8]$ and $\mathbb{R}[Q]$ are not.

Proof. We know that

$$\mathbb{C}[D_8] \simeq \bigoplus_{j=1}^{5} \mathrm{End}_{\mathbb{C}}\left(V_j\right) \simeq \bigoplus_{j=1}^{5} M_{d_j}(\mathbb{C}),$$

with similar for $\mathbb{C}[Q]$. But recall that D_8 and Q have "identical" character tables, namely they have the same number of irreducible complex representations with the same distribution of dimensions, hence it follows by this characterization that the group rings are isomorphic. ■

↪**Proposition 2.6**: Let D_8 be the dihedral group on 4 elements and Q the group of quaternions. Show that the group rings $\mathbb{C}[D_8]$ and $\mathbb{C}[Q]$ are isomorphic, but the groups rings $\mathbb{R}[D_8]$ and $\mathbb{R}[Q]$ are not.

Proof. Recall from proving that the number of irreducible representations is equal to the number of conjugacy classes of a group, we know

$$\mathbb{C}[D_8] = \mathrm{End}_{\mathbb{C}}(V_1) \oplus \cdots \oplus \mathrm{End}_{\mathbb{C}}(V_5),$$

where $V_1, \ldots, V_5$ enumerate the irreducible representations; recall that we have four 1-dimensional representations and a final 2-dimensional representations, we find by picking bases for each V_i that

$$\mathbb{C}[D_8] = \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C}).$$

But Q has the same number of irreducible representations with the same dimensions, hence

$$\mathbb{C}[Q] = \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C}),$$

hence the two are isomorphic.

For $\mathbb{R}[D_8]$, recall that all of the representations are real-valued, so we may realize the same type of isomorphism, and fnd

$$\mathbb{R}[D_8] = \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus M_2(\mathbb{R}).$$

However, in Q, all of the representations are real other than the 2-dimensional one, which cannot be realized as a 2-dimensional representation over $\mathbb{R}$; however, as a group ring,

$$\mathbb{R}[Q] = \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{H},$$

where $\mathbb{H}$ the ring of Hamiltonian quaternions. This is a 4-dimensional real-vector space (namely, we can identify it as a subspace of $M_4(\mathbb{R})$ by identifying i with $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, j with $\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$, and k with $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$). Hence, these two real-valued group rings cannot be isomorphic. ■

↪**Proposition 2.7**: Write down the character table of the symmetry group $G = S_4$ of the cube. Write the character of the permutation representation of G acting on the 8 vertices of the cube, and use the character table to write this character as a sum of irreducible characters.

Proof. See Table 1 for the character table of G (and its derivation). The character χ_C of the permutation representation is given, for each conjugacy class, the number of fixed points of G acting on the vertices (derived here):

	$1A$	$2A$	$2B$	$3A$	$4A$
χ_C	8	0	0	2	0

To write χ_C as a sum of irreducible characters, take the inner product of χ_C with each irreducible character; one should find

$$\chi_C = \chi_1 + \chi_2 + \chi_4 + \chi_5.$$

■

↪**Proposition 2.8**: Let C be a conjugacy class in a finite group G. Show that the element

$$\alpha_C := \sum_{g \in C} g \in \mathbb{C}[G]$$

belongs to the center of the complex group ring of G. If $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ is an irreducible representation of G, show that the matrix

$$\rho(\alpha_C) := \sum_{g \in C} \rho(g) \in M_n(\mathbb{C})$$

is a scalar matrix and write down the scalar in terms of the character of ρ.

Proof. If suffices to check that α_C commutes with every $h \in G$ since $\mathbb{C}$ is obviously commutative; we find

$$h\alpha_C h^{-1} = \sum_{g \in C} hgh^{-1} = \sum_{\tilde{g} \in C} \tilde{g} = \alpha_C,$$

where the summation remains fixed under the change of indexing $\tilde{g} = hgh^{-1}$, since conjugacy classes are by virtue closed under conjugation.

Next, we can view $\rho(\alpha_C)$ as a homomorphism $V \to V$ where $V = \mathbb{C}^n$ the corresponding vector space representation. In this case, the same proof as above gives that $\rho(\alpha_C)$ actually a G-equivariant homomorphism on V, and so by Schur's Lemma, $\rho(\alpha_C) = \lambda I_n$ for some $\lambda \in \mathbb{C}$. To compute λ, we can compute traces; on the one hand, we have $\mathrm{tr}(\lambda I_n) = n \cdot \lambda$, while also

$$\mathrm{tr}(\rho(\alpha_C)) = \sum_{g \in C} \mathrm{tr}(\rho(\alpha_C)) = \sum_{g \in C} \chi(g) = \#C \cdot \chi(C),$$

where χ the corresponding character of ρ, and where we use the fact that χ constant on conjugacy classes. Comparing these, we conclude $\lambda = \frac{\#C \cdot \chi(C)}{n}$; noting that $n = \chi(1)$, then

$$\rho(\alpha_C) = \frac{\#C \cdot \chi(C)}{\chi(1)} I_n.$$

■

↪**Proposition 2.9**: State Maschke's Theorem about complex finite dimensional representations of finite groups. Give a counterexample to illustrate that it can fail to be true when $G = \mathbb{Z}$ is the infinite cyclic group.

Proof. See Thm. 1.2 for the statement. The typical counter example is the two-dimensional representation of $\mathbb{Z}$ given by $n \mapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. One can show that while $\mathbb{C} \cdot e_1$ an irreducible one-dimensional subspace, there is no complementary irreducible one-dimensional space. ■

↪**Proposition 2.10**: Let $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ be the Quaternion group of order 8. What are the dimensions of the irreducible representations of Q? Realize the abstract group Q as a "concrete" group of matrices with complex entries.

Proof. There are 4 irreducible representations of dimension 1, and a unique (faithful) irreducible representation of dimension 2 (the first four can be found by modding out the center of Q which gives a homomorphism to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2$; the last can be found by just computing orthogonality relations).

The "concrete" realization, as a subgroup of $\mathrm{GL}_2(\mathbb{C})$, is given by $1 \leftrightarrow I_2$, $-1 \leftrightarrow -I_2$, and

$$i \leftrightarrow \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad j \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad k \leftrightarrow \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix},$$

with $-i, -j, -k$ defined in the obvious way (this, of course, up to conjugation of every element; this certainly isn't unique). ■

↪**Proposition 2.11**: Let C_1, C_2, C_3 be three conjugacy classes in a finite group G, and let $N(C_1, C_2, C_3)$ be the number of solutions to the equation $g_1 g_2 g_3 = 1$ with $g_j \in C_j$ (with $1 \leq j \leq 3$). Show that

$$N(C_1, C_2, C_3) = \frac{\#C_1 \#C_2 \#C_3}{\#G} \sum_{\chi} \frac{\chi(C_1)\chi(C_2)\chi(C_3)}{\chi(1)},$$

where the sum is taken over the irreducible characters χ of G, and $\chi\left(C_j\right)$ is a notation for $\chi(g)$ with g any element of C_j.

Proof. (A First Proof) The key observation is to notice that, using the notations of 3 questions ago, consider the element $\alpha_{C_1}\alpha_{C_2}\alpha_{C_3} \in \mathbb{C}[G]$;one notices that the coefficient of this element corresponding to the identity in G is equal to $N(C_1, C_2, C_3)$. We'd like to "pick out" this element, which we can do by taking the inner product of the element with χ_{reg}, the character of the regular representation; this gives on the one hand

$$\chi_{\mathrm{reg}}\left(\alpha_{C_1}\alpha_{C_2}\alpha_{C_3}\right) = \#G \cdot N(C_1, C_2, C_3).$$

On the other hand, we know that $\chi_{\mathrm{reg}} = \sum_{\chi} \chi(1) \cdot \chi$, where the summation ranges over the irreducible representations of G; so, it suffices to find the character of $\alpha_{C_1}\alpha_{C_2}\alpha_{C_3}$ on each representation. If ρ an irreducible representation with character χ, then using three questions ago, we find

$$\begin{aligned}\chi\left(\alpha_{C_1}\alpha_{C_2}\alpha_{C_3}\right) &= \operatorname{tr}\left(\rho\left(\alpha_{C_1}\right)\rho\left(\alpha_{C_2}\right)\rho\left(\alpha_{C_3}\right)\right)\\ &= \operatorname{tr}\left(\frac{\#C_1\cdot\chi(C_1)}{\chi(1)}\cdot\frac{\#C_2\cdot\chi(C_2)}{\chi(1)}\cdot\frac{\#C_3\cdot\chi(C_3)}{\chi(1)}I_{\chi(1)}\right)\\ &= \#C_1\#C_2\#C_3\frac{\chi(C_1)\chi(C_2)\chi(C_3)}{\chi(1)^2}.\end{aligned}$$

Hence, we find that

$$\begin{aligned}\#G\cdot N(C_1,C_2,C_3) &= \chi_{\text{reg}}\left(\alpha_{C_1}\alpha_{C_2}\alpha_{C_3}\right)\\ &= \sum_{\chi}\chi(1)\chi\left(\alpha_{C_1}\alpha_{C}\right)\\ &= \#C_1\#C_2\#C_3\sum_{\chi}\frac{\chi(C_1)\chi(C_2)\chi(C_3)}{\chi(1)},\end{aligned}$$

giving the answer upon dividing both sides by $\#G$. ■

Proof. (A Second Proof) Recall the isomorphism of rings

$$\underline{\rho} = (\rho_1,\ldots,\rho_h) : \mathbb{C}[G] \to \bigoplus_{i=1}^{h}\operatorname{End}_{\mathbb{C}}(V_i),$$

developed earlier to find the number of irreducible characters of a group. From question 2., we know that

$$\begin{aligned}\underline{\rho}\left(\alpha_{C_1}\alpha_{C_2}\alpha_{C_3}\right) &= \left(\rho_1\left(\alpha_{C_1}\right)\rho_1\left(\alpha_{C_2}\right)\rho_1\left(\alpha_{C_3}\right),\ldots,\rho_h\left(\alpha_{C_1}\right)\rho_h\left(\alpha_{C_2}\right)\rho_h\left(\alpha_{C_3}\right)\right)\\ &= \left(\#C_1\#C_2\#C_3\frac{\chi_1(C_1)\chi_1(C_2)\chi_1(C_3)}{\chi_1(1)}I_{\chi_1(1)},\ldots,\#C_1\#C_2\#C_3\frac{\chi_h(C_1)\chi_h(C_2)\chi_h(C_3)}{\chi_{g(1)}}I_{\chi_h(1)}\right)\\ &= \#C_1\#C_2\#C_3\cdot\left(\frac{\chi_1(C_1)\chi_1(C_2)\chi_1(C_3)}{\chi_1(1)}I_{\chi_1(1)},\ldots,\frac{\chi_h(C_1)\chi_h(C_2)\chi_h(C_3)}{\chi_{g(1)}}I_{\chi_h(1)}\right),\end{aligned}$$

where χ_i the character of ρ_i. Restricting to the vector space structure of $\mathbb{C}[G]$, we know that $\mathbb{C}[G]\simeq L^2(G)$, the space of complex-valued functions on G. Then, notice that $N(C_1,C_2,C_3)$ is the coefficient of $\alpha_{C_1}\alpha_{C_2}\alpha_{C_3}$ corresponding to 1 in the group ring, or, viewing this element as a function, call it f, in $L^2(G)$, the value of $f(1)$. $L^2(G)$ is endowed with a natural inner product, and we can find $f(1)$ by taking the inner product of f with the function $\delta_1 : G\to\mathbb{C}$ given by $\delta_1(g) = \begin{cases}1 \text{ if } g=\text{id}\\ 0 \text{ else}\end{cases}$, which gives

$$\langle f,\delta_1\rangle = \frac{1}{\#G}\cdot f(1).$$

On the other hand, there is a corresponding natural inner product on the vector space $\bigoplus_{i=1}^{h}\operatorname{End}_{\mathbb{C}}(V_i)$. Namely, on each space $\operatorname{End}_{\mathbb{C}}(V_i)$, the natural inner product is

$$\langle A,B\rangle_* := \operatorname{tr}(AB^*),$$

where B^* denotes the conjugate transpose of B. Then, the inner product on the direct sum of the spaces is given by the sum such inner products on each component, i.e. given $A=(A_1,\ldots,A_h), B=(B_1,\ldots,B_h)$, we define

$$\langle A, B\rangle_+ := \sum_{i=1}^{h} \operatorname{tr}(A_i B_i^*).$$

I claim that this inner product is "equivalent" to the original one on $L^2(G)$. Namely, given $f_1, f_2 \in L^2(G)$, note that $\rho_i(f_2)^* = \overline{\rho_i(f_2)} = \rho_i\left(f_2^{-1}\right)$, so we find

$$\begin{aligned}
\langle \underline{\rho}(f_1), \underline{\rho}(f_2)\rangle_+ &= \sum_{i=1}^{h} \operatorname{tr}\left(\rho_i(f_1)\rho_i(f_2)^*\right) \\
&= \sum_{i=1}^{h} \operatorname{tr}\left(\rho_i(f_1)\rho_i\left(f_2^{-1}\right)\right) \\
&= \sum_{i=1}^{h} \operatorname{tr}\left(\rho_i\left(f_1 f_2^{-1}\right)\right) \\
&= \sum_{\chi} \chi\left(f_1 f_2^{-1}\right)
\end{aligned}$$

Finally, notice that

$$\underline{\rho}(\delta_1) = (\rho_1(1), \ldots, \rho_h(1)) = \left(I_{\chi_1(1)}, \ldots, I_{\chi_h(1)}\right)$$

From which we find

$$\begin{aligned}
\langle \underline{\rho}(f), \underline{\rho}(\delta_1)\rangle_+ &= \sum_{i=1}^{h} \operatorname{tr}\left(\#C_1 \#C_2 \#C_3 \frac{\chi_i(C_1)\chi_i(C_2)\chi_i(C_3)}{\chi_i(1)} I_{\chi_i(1)}\right) \\
&= \sum_{\chi} \#C_1 \#C_2 \#C_3 \cdot \chi(C_1)\chi(C_2)\chi(C_3)
\end{aligned}$$

■

§3 Galois Theory

The original motivation of Galois Theory was the study of polynomial equations and so-called "solvability by radicals". More modernly, the motivation is in the study of fields via their symmetries.

One original question was with solving the cubic equation, $ax^3 + bx^2 + cx + d = 0$. We outline the proof here. Without loss of generality, one assumes $a = 1$ and $b = 0$, by dividing by a (if $a = 0$, this reduces to a quadratic) and making an appropriate summation. This gives the so-called "depleted cubic" equation, we write

$$x^3 + px + q = 0.$$

Writing $x = u + v$, we find

$$\begin{gathered}
(u+v)^3 + p(u+v) + q = 0 \\
\Rightarrow u^3 + v^3 + 3uv(u+v) + p(u+v) + q = 0 \\
\Rightarrow \left[u^3 + v^3 + q\right] + (3uv + p)(u+v) = 0;
\end{gathered}$$

then, if $u^3 + v^3 + q = 0$ and $3uv + p = 0$, we find a solution; namely, we have now a system of two equations

$$\begin{cases} u^3 + v^3 = -q \\ uv = -\frac{p}{3} \end{cases}.$$

Cubing the second, we find

$$\begin{cases} u^3 + v^3 = -q \\ u^3 v^3 = -\frac{p^3}{27} \end{cases},$$

from which we see u^3 and v^3 are solutions to a quadratic equation

$$x^2 + qx - \frac{p^3}{27} = 0;$$

this equation is often called the "quadratic resolvent" of the cubic. Hence, by applying the quadratic formula, we know

$$u^3, v^3 = \frac{-q \pm \sqrt{p^2 + 4p^3/27}}{2}$$

so

$$u, v = \sqrt[3]{\frac{-q \pm \sqrt{p^2 + 4p^3/27}}{2}}.$$

Substituting back to our original expression, we find our general solution

$$x = \sqrt[3]{\frac{-q + \sqrt{p^2 + 4p^3/27}}{2}} + \sqrt[3]{\frac{-q - \sqrt{p^2 + 4p^3/27}}{2}}$$

to the cubic equation. One notices that this should give 9 solutions (3 cube roots exists, for each cube root), and in general gives complex numbers. We'll discuss the implications of this to follow.

There is a similar formula for the general quartic equation, involving square, cube, and fourth roots, with a similar method leading to a resolvent cubic. However, attempting the same method for the quintic equation leads to a resolvent sextic equation, which is clearly no help at all. We'll see that this is intimately tied to the symmetries, namely, the symmetry groups, of the roots of the respective polynomials.

§3.1 Field Extensions

↪**Definition 3.1** (Field Extension): If E and F are fields, we say E is an extension of F if F is a subfield of E; we'll often denote E/F.

Note that if E an extension of F, then E is also a vector space over F (by "forgetting" the multiplication).

↪**Definition 3.2** (Degree): The *degree* of E over F is the dimension of E as an F vector space, often denoted $[E:F] = \dim_F(E)$. We call then E a *finite* extension of F if $[E:F] < \infty$.

⊛ **Example 3.1**:

1. Consider $E = \mathbb{C}$ and $F = \mathbb{R}$, then $[E:F] = 2$ (with, for instance, basis $\{1, i\}$).
2. Consider $E = \mathbb{C}$ and $F = \mathbb{Q}$, then $[E:C] = \infty$.
3. Let F be any field and let $E = F[x]/(p(x))$ where $p(x)$ irreducible, hence E is a field itself. E an extension of F, since F can be realized as a subfield via the constant polynomials in E. Then, $[E:F] = \deg(p(x))$.
4. Let $E = F(x) =$ fraction field of $F[x] = \left\{\frac{f(x)}{g(x)} \mid f, g \in F[x], g \neq 0\right\}$. By similar reasoning to 3., this also an extension of F, but now $[E:F] = \infty$ (for instance, $\{x^n : n \in \mathbb{N}\}$ is an infinite, linearly independent subset of E).

↪**Theorem 3.1** (Multiplicativity of Degree): Given finite extensions $K \subset F \subset E$, we have

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

Proof. Put $n := [E:F], m := [F:K]$. Let $\alpha_1, \ldots, \alpha_n$ be a basis for E as an F-vector space and $\beta_1, \ldots, \beta_m$ a basis for F as a K-vector space. Now, notice that if $a \in E$, then

$$a = \lambda_1\alpha_1 + \ldots + \lambda_n\alpha_n,$$

for $\lambda_i \in F$. Then, λ_i may be viewed as elements of the vector space F over K, so we may write

$$\lambda_i = \lambda_{i1}\beta_1 + \cdots + \lambda_{im}\beta_m,$$

for some $\lambda_{ij} \in K$. Hence,

$$\begin{aligned} a &= (\lambda_{11}\beta_1 + \cdots + \lambda_{1m}\beta_m)\alpha_1 + (\lambda_{21}\beta_1 + \ldots + \lambda_{2m}\beta_m)\alpha_2 + \cdots + (\lambda_{n1}\beta_1 + \cdots + \lambda_{nm}\beta_m)\alpha_n \\ &= \sum_{1\le i\le n}\sum_{1\le j\le m} \lambda_{ij}\alpha_i\beta_j. \end{aligned}$$

Since the representation in each basis $\{\alpha_i\}, \{\beta_j\}$ was unique, it must be that this representation also unique. Thus, $\{\alpha_i\beta_j\}_{\substack{1\le i\le n \\ 1\le j\le m}}$ is a K-basis for E, so $\dim_K(E) = m \cdot n = \dim_F(E) \cdot \dim_K(F)$. ∎

§3.2 Ruler and Compass Constructions

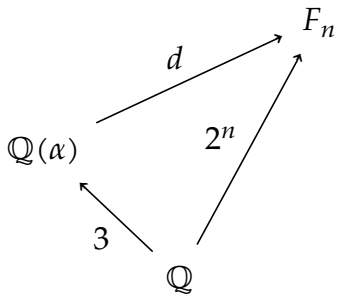
↪**Definition 3.3**: A complex number is said to be *constructible by ruler and compass* if it can be obtained from $\mathbb{Q}$ by successive applications of the field operations plus extractions of square roots.

The set of elements constructible by ruler and compass is an extension of $\mathbb{Q}$ of infinite degree. Namely, each extraction of a square root can be abstractly realized as adjoining a square root of an element, say a, that doesn't have a rational square root to $\mathbb{Q}$, which forms a field extension $\mathbb{Q}(\sqrt{\alpha})$. We can repeat this process, adjoining new elements and constructing further extensions. A number is then solvable by constructible by ruler and compass if it is contained in some field extension of $\mathbb{Q}$ obtained via some finite number of adjoinments of square roots.

↪**Theorem 3.2**: If $\alpha \in \mathbb{R}$ is the root of an irreducible cubic polynomial over $\mathbb{Q}$, then α is *not* constructible by ruler and compass.

Proof. Suppose otherwise, that α is constructible. Then, there exists fields $\mathbb{Q} \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n$ with $[F_{i+1} : F_i] = [F_1 : \mathbb{Q}] = 2$ for each i (namely, $F_{i+1} = F_i(\sqrt{a_i})$ for some a_i in F_i such that $\sqrt{a_i} \notin F_i$). Hence, by multiplicativity we know $[F_n : \mathbb{Q}] = 2^n$. On the other hand, if p the irreducible (over $\mathbb{Q}$) cubic polynomial for which α is a root, $\mathbb{Q}(\alpha) = \mathbb{Q}[x]/p(x)$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

So, it must be that F_n an extension of $Q(\alpha)$ so $[F_n : \mathbb{Q}(\alpha)] = d \in \mathbb{N}$, but by multiplicativity, $3d = 2^n$ which is impossible.



■

⊛ **Example 3.2**:
1. $p(x) = x^3 - 2$ has root $\alpha = \sqrt[3]{2}$ ("duplicating the cube").
2. $p(x) = 4x^3 + 3x + \frac{1}{2}$ has root $r = \cos\left(\frac{2\pi}{9}\right)$ ("trisection of the angle").

§3.3 Automorphisms of Field Extensions

↪**Definition 3.4** (Algebraic): An element α in an extension E over F is said to be *algebraic* if it is the root of a polynomial $f \in F[x]$.

⊛ **Example 3.3**: $\sqrt{2}, i$ are algebraic over Q, but π, for instance, is not. In fact, one can show the set of algebraic numbers in $\mathbb{R}$ over $\mathbb{Q}$ is countable.

↪**Lemma 3.1**: If E a finite extension of F, any α in E is algebraic.

Proof. Put $n := [E : F]$ and let $\alpha \in E$. Then, $\{1, \alpha, ..., \alpha^n\}$ must be a linearly dependent subset of E, hence there must exist scalars $a_i \in F$ such that $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Letting $f(x) = a_0 + a_1x + \cdots + a_nx^n$ completes the proof. ■

↪**Definition 3.5** (Automorphisms of a Field Extension): The automorphism group of E/F is defined as the group

$$\mathrm{Aut}(E/F) = \left\{ \sigma : E \to E \;\middle|\; \begin{array}{c} \sigma(x+y) = \sigma(x) + \sigma(y) \\ \sigma(xy) = \sigma(x)\sigma(y) \\ \sigma|_F = \mathrm{id} \end{array} \right\}.$$

In particular, $\sigma \in \mathrm{Aut}(E/F)$ respects the field structure on E, and leaves the distinguished subfield F in E invariant.

Remark 3.1: Note that an automorphism is a bijection $E \to E$ which is a homomorphism of rings. In particular, any homomorphism $\varphi : E \to E$ is automatically injective, so if $[E : F] < \infty$, φ injective $\Leftrightarrow$ φ surjective. Hence we need not specify this condition in the definition above.

↪**Corollary 3.1**: $\sigma(1) = 1$, $\sigma(0) = 0$ and $\sigma\left(a^{-1}\right) = \sigma(a)^{-1}$ for $\sigma \in \mathrm{Aut}(E/F)$.

↪**Proposition 3.1**: If $[E : F] < \infty$, $\mathrm{Aut}(E/F)$ cats on E with finite orbits.

Proof. Let $\alpha \in E$, and $f(x) = a_nx^n + \cdots + a_1x + a_0$ a polynomial with coefficients in F such that $f(\alpha) = 0$, which exists since α must be algebra since $[E : F] < \infty$. Then, notice that

$$\sigma(f(\alpha)) = \sigma(0) = 0$$

on the one hand, while also

$$\sigma(f(\alpha)) = \sigma(a_n\alpha^n + \cdots + a_1\alpha + a_0) = a_n\sigma(\alpha)^n + \cdots + a_1\sigma(\alpha) + a_0 = f(\sigma(\alpha)),$$

using each of the defining axioms of $\mathrm{Aut}(E/F)$. Hence, $\sigma(\alpha)$ also a root of f, and thus

$$\mathrm{Orb}_{\mathrm{Aut}(E/F)}(\sigma) \subset \{\text{roots of } f \text{ in } E\},$$

which is a finite set, since f has finite degree n hence at most n roots. Thus, $\mathrm{Orb}_{\mathrm{Aut}(E/F)}(\sigma)$ must also be finite. ■

Remark 3.2: Notice that we only used the fact that α was algebraic, not the full scope of the finiteness of E/F. In fact, the same proof applies when E/F "algebraic", namely when every element of E algebraic.

↪**Theorem 3.3**: If $[E : F] < \infty$, then $\#\operatorname{Aut}(E/F) < \infty$.

Proof. Let $\alpha_1, ..., \alpha_n$ generate E over F so $E = F(\alpha_1, ..., \alpha_n)$. Then if $\sigma \in \operatorname{Aut}(E/F)$, it is completely determined by the n-tuple $(\sigma\alpha_1, ..., \sigma\alpha_n)$. By the previous proof, we know that

$$(\sigma\alpha_1, ..., \sigma\alpha_n) \subseteq \operatorname{Orb}_G(\alpha_1) \times \cdots \times \operatorname{Orb}_G(\alpha_n),$$

where $G := \operatorname{Aut}(E/F)$. The set on the RHS is finite by the previous proof, and thus σ is determined by a finite amount of "data", and thus there can exist only finitely many σ's. ■

⊛ **Example 3.4**: If E/F generated by a single element α (so $E = F(\alpha)$), let $p(x) \in F[x]$ be the minimal polynomial of α. Then, $F(\alpha) \simeq F[x]/(p(x))$, so $[F(\alpha) : F] = \deg(p(x))$. Then, $\sigma \in \operatorname{Aut}(F(\alpha)/F)$ completely determined by $\sigma(\alpha) \in \{\text{roots of } p(x)\}$. This set has cardinality at most $\deg(p(x)) = [F(\alpha) : F]$; thus,

$$\#\operatorname{Aut}(E/F) \leq [E : F].$$

We'll see this holds more generally.

↪**Theorem 3.4**: If E/F is any finite extension of fields, then $\#\operatorname{Aut}(E/F) \leq [E : F]$.

Proof. We prove by induction on the number of generators of E over F. Namely, we write $E = F(\alpha_1, ..., \alpha_n)$.

Let M be any extension of F, fixed. We'll consider the space $\operatorname{Hom}_F(E, M)$, and we'll prove the slightly stronger statement that $\#\operatorname{Hom}_F(E, M) \leq [E : F]$, which proves the desired result by setting $M = E$.

Consider $n = 1$. Then, $E = F(\alpha) = F[\alpha]$, so

$$[E : F] = \deg p_\alpha(x) =: d,$$

where $p_\alpha(x)$ the minimal degree polynomial in $F[x]$ that is satisfied by α. Then, any φ in the space of interest $\operatorname{Hom}_F(E, M)$ is completely determined by the image of α. In particular, if $p_\alpha(x) = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1}$, then

$$0 = \varphi(0) = \varphi(p_\alpha(\alpha)) = a_0 + a_1\varphi(\alpha) + \cdots + a_{d-1}\varphi(\alpha)^{d-1} = 0,$$

so, the map $\varphi \mapsto \varphi(\alpha)$ is an inclusion $\operatorname{Hom}_F(E, M) \to \{\text{roots of } p_\alpha(x)\}$. Since the set on the right is a set of size at most d, the proof follows.

Suppose now the case for n and let $E = F(\alpha_1, ..., \alpha_{n+1})$, and let $F' = F(\alpha_1, ..., \alpha_n)$. If $F' = E$, we're done. Else, we have the set-up,

$$F \text{—}^{d_1} F' = F(\alpha_1, ..., \alpha_n) \text{—}^{d_2} E = F'(\alpha_{n+1}).$$

Let $g(x) \in F'[x]$ be the minimal polynomial of α_{n+1}, so $d_2 = \deg g(x)$. Consider the restriction map

$$\mathrm{Hom}_F(E, M) \to \mathrm{Hom}_F(F', M).$$

By the induction hypothesis, since F' generated by n elements, we have $\#\mathrm{Hom}_F(F', M) \leq d_1 = [F' : F]$. Now, give $\varphi_0 \in \mathrm{Hom}_F(F', M)$, we'd like to compute how many $\varphi' : E \to M$ such that $\varphi|_{F'} = \varphi_0$. Really, then, we need to consider how many options there are of $\varphi(\alpha_{n+1})$. We know that α_{n+1} is a root of $g(x) = \lambda_{d_2} x^{d_2} + \cdots + \lambda_1 x + \lambda_0$ where $\lambda_j \in F'$. Then,

$$0 = \varphi(g(\alpha_{n+1})) = \varphi\left(\lambda_{d_2}\right)\varphi(\alpha_{n+1})^{d_2} + \cdots + \varphi(\lambda_1)\varphi(\alpha_{n+1}) + \varphi(\lambda_0).$$

However, note that λ_{d_2} not in F so φ not constant on the λ_i's, as in the previous case. However, we can write then

$$= \varphi_0\left(\lambda_{d_2}\right)\varphi(\alpha_{n+1})^{d_2} + \cdots + \varphi_0(\lambda_1)\varphi(\alpha_{n+1}) + \varphi_0(\lambda_0),$$

so $\varphi(\alpha_{n+1})$ is a root of the polynomial "$\varphi_0(g(x)) \in M[x]$", by which we mean the polynomial $g(x)$ with the coefficients evaluated on φ_0. There are at most d_2 choices of roots of this new polynomial, hence at most d_2 choices for $\varphi(\alpha_{n+1})$. Thus, we find

$$\#\mathrm{Hom}_F(E, M) \leq d_1 \cdot d_2 = [E : F],$$

by multiplicativity of the degrees. ■

↪**Definition 3.6** (Galois): An extension E/F is said to be *Galois* if $\#\,\mathrm{Aut}(E/F) = [E : F]$, in which case we write $\mathrm{Gal}(E/F) = \mathrm{Aut}(E/F)$.

⊛ **Example 3.5**: Let $E = \mathbb{C}$ and $F = \mathbb{R}$ so $[E : F] = 2$. Then, the conjugation map

$$c : \mathbb{C} \to \mathbb{C}, \qquad x + iy \mapsto \overline{x + iy} = x - iy$$

is an automorphism of $\mathbb{C}/\mathbb{R}$. So,

$$\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{1, c\};$$

there couldn't possible be any more maps else the previous upper bound would be contradicted.

⊛ **Example 3.6**: Let $F = \mathbb{Q}$ and $E = \mathbb{Q}\left(\sqrt[3]{2}\right) = \mathbb{Q}[x]/\left(x^3 - 2\right)$. We can also consider this as a subfield of $\mathbb{R}$ by identifying $\sqrt[3]{2}$ with the distinct real cube root of 2. Then,

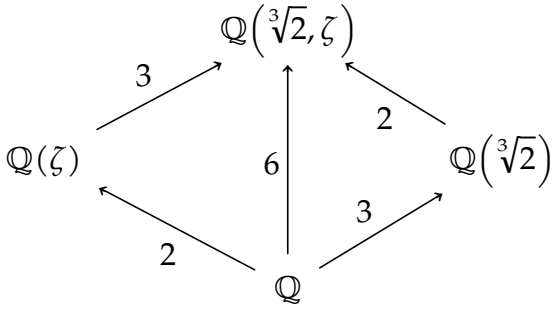
$$\mathrm{Aut}\left(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}\right) \leftrightarrow \left\{\text{roots of } x^3 - 2 \text{ over } \mathbb{Q}\left(\sqrt[3]{2}\right)\right\},$$

since $\sqrt[3]{2}$ must be mapped to another element which cubes to 3. However, there is only one such element, namely itself, so the only possible automorphism is the identity and so $\#\,\mathrm{Aut}\left(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}\right) = 1 < 3$.

3.3.1 A Thorough Example

Consider now $F = \mathbb{Q}$ and $E = \mathbb{Q}\left(\sqrt[3]{2}, \zeta\right)$ where $\zeta^3 = 1$ (but is not 1) so ζ satisfies the quadratic equation $x^2 + x + 1$; so, we can realize $\mathbb{Q}\left(\sqrt[3]{2}, \zeta\right) \subset \mathbb{C}$. Moreover, note that $\left[\mathbb{Q}\left(\sqrt[3]{2}, \zeta\right) : \mathbb{Q}\right] = 6$; we have as basis $\left\{1, \sqrt[3]{2}, \sqrt[3]{2}^2, \zeta, \zeta\sqrt[3]{2}, \zeta\sqrt[3]{2}^2\right\}$.

Alternatively, one can use the multiplicativity of the degree to deduce this number; this "sequence of extensions" is visualized below.



We wish to compute $\#\,\mathrm{Aut}(E/\mathbb{Q})$. Let φ be an automorphism; then, since E generated by $\sqrt[3]{2}$ and ζ, φ is completely determined by what it maps $\sqrt[3]{2}$ and ζ to.

First, $\varphi(\zeta)$ must be a root of the polymomial $x^2 + x + 1$, so there are precisely two possibilities, ζ and $\overline{\zeta}$. Similarly, $\varphi\left(\sqrt[3]{2}\right)$ must be a root of the polynomial $x^3 - 2$ (in E). So, it may of course map to $\sqrt[3]{2}$, but also, since $\zeta^3 = \overline{\zeta}^3 = 1$, $\zeta \cdot \sqrt[3]{2}$ and $\overline{\zeta} \cdot \sqrt[3]{2}$ are also roots of $x^3 - 2$. Hence, there are 2 possibilities for $\varphi(\zeta)$ and 3 for $\varphi\left(\sqrt[3]{2}\right)$, for a total of 6 automorphisms.

We can more concretely determined the group structure of $\mathrm{Aut}(E/\mathbb{Q})$. Being a group of order 6, it must be (isomorphic to) either $\mathbb{Z}/6\mathbb{Z}$ or S_3. We claim it is the second case. The easiest way to show this is that $\mathrm{Aut}(E/\mathbb{Q})$ can be made to act transitively on a set of 3 elements. Let $r_1 = \sqrt[3]{2}, r_2 = \zeta\sqrt[3]{2}, r_3 = \overline{\zeta}\sqrt[3]{2}$ enumerate the roots of $x^3 - 2$ in E. Then, the automorphisms in $\mathrm{Aut}(E/\mathbb{Q})$ have a natural induced action on the roots. We can tabulate the possibilities; across the top, we write what ζ is mapped to by a given φ, and across the left we write what $\sqrt[3]{2}$ is mapped to:

	$\zeta \to \zeta$	$\zeta \to \overline{\zeta}$
$\sqrt[3]{2} \to \sqrt[3]{2}$	id	$(r_2 r_3)$

$\sqrt[3]{2} \to \zeta\sqrt[3]{2}$	$(r_1 r_2 r_3)$	$(r_1 r_2)$
$\sqrt[3]{2} \to \zeta\sqrt[3]{2}$	$(r_1 r_3 r_2)$	$(r_1 r_3)$

To compute these, consider for instance the φ such that $\varphi(\zeta) = \zeta$ and $\varphi\left(\sqrt[3]{2}\right) = \zeta\sqrt[3]{2}$. Then, $\varphi(r_1) = r_2$, and

$$\varphi(r_2) = \varphi\left(\zeta\sqrt[3]{2}\right) = \varphi(\zeta)\varphi\left(\sqrt[3]{2}\right) = \zeta\zeta\sqrt[3]{2} = \overline{\zeta}\sqrt[3]{2} = r_3,$$

and finally

$$\varphi(r_3) = \varphi\left(\overline{\zeta}\right)\varphi\left(\sqrt[3]{2}\right) = \overline{\zeta}\zeta\sqrt[3]{2} = \sqrt[3]{2} = r_1,$$

so, φ acts as the 3-cycle $(r_1 r_2 r_3)$ on the set of roots.

Hence, we conclude that

$$\mathrm{Aut}(E/\mathbb{Q}) = \mathrm{Gal}(E/\mathbb{Q}) = S_3.$$

§3.4 Properties of Galois Extensions

Throughout, we assume E/F a finite Galois extension, and we put $G = \mathrm{Gal}(E/F)$.

Denote by $E^G = \{\alpha \in E \mid g\alpha = \alpha \ \forall\, g \in G\}$ the set of fixed points of E under G.

↪**Proposition 3.2**: E^G is a subfield of E which contains F, so we have the inclusion of extensions $E \supset E^G \supset F$.

Proof. If $x, y \in E$ are fixed under G, then $g(x+y) = gx + gy = x + y$, with a similar computation for products. So, E^G closed under addition, multiplication and is moreover a subfield.

For the second claim, note that by definition, automorphisms of E/F are constant on elements of F, so certainly $F \subset E^G$. ■

↪**Theorem 3.5**: $E^G = F$.

Proof. We have

$$E — E^G — F,$$

of extensions. Consider now $\mathrm{Aut}\left(E/E^G\right)$. This certainly contains G as a subgroup. We know then

$$[E : F] = \#G \leq \#\ \mathrm{Aut}\left(E/E^G\right) \leq \left[E : E^G\right].$$

But we know that $\left[E : E^G\right]$ divides $[E : F]$ by multiplicativity, so we conclude that $\left[E : E^G\right] = [E : F]$ hence $\left[E^G : F\right] = 1$. Thus, $E^G = F$. ■

↪**Theorem 3.6**: If $f(x)$ is an irreducible polynomial in $F[x]$ which has a root in E, then $f(x)$ splits completely into linear factors in $E[x]$.

More generally for non-Galois groups, if an extension has this property, we say E/F is normal.

PROOF. Let $r \in E$ be a root of $f(x)$. Let $\{r_1, ..., r_n\}$ be the orbit of r under the action of G and consider the polymomial

$$g(x) = (x - r_1)(x - r_2)\cdots(x - r_n)$$
$$= x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + \cdots + (-1)^n \sigma_n \in E[x],$$

where $\sigma_1, ..., \sigma_n$ are the so-called "elementary symmetric functions" in $r_1, ..., r_n$. Namely,

$$\begin{aligned}
\sigma_1 &= r_1 + \cdots + r_n, \\
\sigma_2 &= r_1 r_2 + r_2 r_3 + \cdots + r_{n-1} r_n = \sum_{1 \le i < j \le n} r_i r_j \\
\sigma_3 &= \sum_{1 \le i < j < k \le n} r_i r_j r_k, \\
&\vdots \\
\sigma_n &= r_1 \cdots r_n.
\end{aligned}$$

Remark that each σ_i invariant under permutations of the r_i's. Hence, in particular, $\sigma_i \in E^G$; by construction, the r_i's were defined as the orbit of our original root r under the action of G i.e. G acts on the set $\{r_1, ..., r_n\}$ by permutation. So, the expression σ_i is an element of E, which is invariant under the action of G and so by definition in E^G. But remember, E/F Galois thus $E^G = F$ so each $\sigma_i \in F$.

In particular, then, $g(x)$ a polynomial with coefficients in F so $g(x) \in F[x]$. Remember our original $f(x)$ is irreducible in $F[x]$ so namely is the minimal irreducible polymomial on r over F; any other polymomial that vanishes on r must be divisible by f, hence $f(x) | g(x)$, from which we conclude $f(x)$ factors completely into linear factors in $E[x]$. ■

§3.5 Splitting Fields

Let F be a field and $f(x) \in F[x]$.

↪**Definition 3.7** (Splitting Field): A *splitting field* of $f(x)$ is an extension E/F satisfying:

1. $f(x)$ factors into linear factors in $E[x]$, namely,
$$f(x) = (x - r_1)\cdots(x - r_n)$$
for $r_i \in E$;
2. E is generated as a field by the roots $r_1, ..., r_n$.

3.5.1 Construction of a Splitting Field

We'll construct a splitting field by induction on $\deg(f(x)) = n$. If $n = 1$, there's nothing to do and $E = F$. Let then $\deg(f(x)) = n + 1$ and let $p(x)$ be an irreducible factor of $f(x)$. Then, let

$$L := F[x]/(p(x)).$$

L a field, since p irreducible, and it contains a root of $p(x)$ and hence by $f(x)$, by construction. Let r be the root of $p(x)$ in L; namely, recall that $r = x + (p(x))$. Then, $x - r$ divides $f(x)$ in $L[x]$, so $f(x) = (x - r)g(x)$ for some g of degree n. By the induction hypothesis, we can construction E to be a splitting field of $g(x)$ over L; then, in particular, f also splits over E, so E also a splitting field of f, completing the construction.

Pictorally, viewing L as F adjoining a root r_1 of f, we have:

$$\begin{array}{cc} L_N & (x - r_1)(x - r_2)\cdots(x - r_N) = f(x) \\ \uparrow & \\ \vdots & \\ \uparrow & \\ L_2 = L(r_2) & (x - r_2)h(x) = g(x) \\ \uparrow & \\ L = F(r_1) & (x - r_1)g(x) = f(x) \\ \uparrow & \\ F & f(x) \end{array}$$

Noting that, by virtue, this process terminates after finitely many iterations since f of fintie degree.

Remark 3.3: It's very hard to compute the degree of a splitting field of $f(x)$, since at each iteration of the construction several, or just a single, new root of the polynomial will be adjoined.

In particular, if $f(x)$ is irreducible of degree n and E the splitting field of $f(x)$, then

$$n \leq [E : F] \leq n!.$$

The lower bound comes from the fact that we need to adjoin at least one root of f to F to get to E; if a single adjointment suffices to include all the roots of f, then $[E : F] = n$. The upper bound comes from the "worst-case", where the first root adjoinment adds no other roots of f to $F(r_1)$, and $f(x) = (x - r_1)g(x)$ where g irreducible over $F(r_1)$, and this repeats at each iteration (at each stage, only exactly one root is added). In this case, $[E : F] = [E : F(r_n)] \cdot [F(r_n) : F(r_{n-1})]\cdots[F(r_1) : F] = n!$.

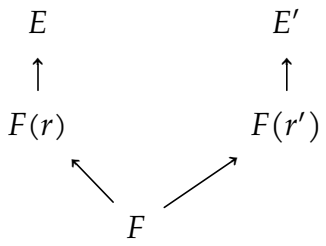
§3.6 Properties of a Splitting Field

↪**Theorem 3.7**: If $f(x) \in F[x]$ and E, E' are splitting fields of $f(x)$ over F, then E and E' are isomorphic as extensions of F i.e. there is an isomorphisms of fields between E and E' that is contant on F.

Proof. We proceed by induction on $n = \deg(f(x))$.

If $n = 1$, then $E = E' = F$.

Suppose the case for all polynomials of degree n and take f a polynomial of degree $n+1$. Let $p(x)$ be an irreducible factor of $f(x)$ and let r be a root of $p(x)$ in E, r' a root of $p(x)$ in E'. Then, we have the "inclusion of fields":



We know then that $F(r)$ and $F(r')$ are isomorphic, since $F(r) = F[x]/(p(x)) = F(r')$ Let φ be an isomorphism from $F(r)$ to $F(r')$.

Let $L = F(r) \overset{\varphi}{=} F(r')$, so E, E' are both extensions of L. Then, E and E' are both splitting fields of $g(x)$ where $g(x)(x - r) = f(x)$. By the induction hypothesis, then, E, E' are isomorphic as extensions of L. ■

Remark 3.4: This theorem establishes a type of uniqueness of splitting fields, up to isomorphism. However, remark that in constructing our isomorphism, we had to pick, arbitrarily, roots r, r' and "identify" them, so to speak. There is no canonical or natural way to pick such roots. Hence, while the two splitting fields E, E' are isomorphic, the possible isomorphism between them is not unique.

↪**Proposition 3.3**: If E/F is Galois, then E is the splitting field of a polynomial $f(x) \in F[x]$.

Proof. Since $[E : F] < \infty$, let $\alpha_1, ..., \alpha_n$ be a finite set of generators for E over F. Let $f_1, ..., f_n$ be irreducible polynomials in $F[x]$ having $\alpha_1, ..., \alpha_n$ as roots. Let $f(x) = f_1(x)f_2(x)\cdots f_n(x)$. By normality, all the f_j's factor completely in $E[x]$, hence so does f. So, the roots of $f(x)$ generate E/F so E is the splitting field of $f(x)$. ■

§3.7 Finite Fields

If F a finite field (a field that is finite as a set), then there is some unique minimal p such that $1 + \cdots + 1 = p \cdot 1 = 0$ (for if no such p existed, F would not be finite). Moreover, p must be prime, for if not then $0 = p = a \cdot b$ for nonzero elements a, b, so a, b are zero divisors in F, which is impossible since F a field. We often denote by $p = \text{char}(F)$, and call then $\mathbb{Z}/p\mathbb{Z} \subset F$ the prime

(sub)field of F. Let $n = \dim_{\mathbb{F}_p}(F)$ be the dimension of F as vector space over this prime field. Then, we conclude $\#F = p^n$; every finite field has cardinality a prime power.

Conversely, given some prime p and some integer n, does there exist an integer n such that $\#F = p^n$? We'll prove this in the affirmative.

↪**Theorem 3.8**: Given a prime p and $n \geq 1$, there is a field of cardinality p^n; in fact, it is unique up to isomorphism.

Proof. Note that if F a field of cardinality p^n, $F^\times$ is an abelian group of cardinality $p^n - 1$. Then, for every $x \in F^\times$, $x^{p^n-1} = 1$, so

$$x^{p^n} - x = 0, \forall\, x \in F = F^\times \cup \{0\}.$$

In particular, F is the collection of roots of the polynomial of $x^{p^n} - x$.

With this in mind, then, for a fixed prime p and integer $n \geq 1$, let F be the splitting field of the polynomial $x^{p^n} - x$ over $\mathbb{F}_p$. We claim that F has cardinality p^n.

Note that $x^{p^n} - x$ has distinct roots in any extension of $\mathbb{F}_p$. Since $f'(x) = -1$ (in the extension), we know that $\gcd(f(x), f'(x)) = 1$ so there are no multiple roots. Hence, $\#F \geq p^n$. Conversely, note that the set of roots of $x^{p^n} - x$ is itself a field; so, $\#F \leq p^n$ and thus $\#F = p^n$.

By the previous section, F being a splitting field of a polynomial, it is unique up to isomorphism, completing the proof of the theorem. ■

A natural extension of this theorem is to ask whether F is Galois over $\mathbb{F}_p$.

↪**Definition 3.8** (Frobenius Homomorphism): The map $\varphi : F \to F$ defined by $\varphi(\alpha) = \alpha^p$ is called the *Frobenius homomorphism* of F.

Because φ is a homomorphism of fields, φ is an injection. φ is also $\mathbb{F}_p$-linear, so φ in particular an automorphism of F. So, $\varphi \in \mathrm{Aut}\left(F/\mathbb{F}_p\right)$. What is the order of φ? We know that

$$\varphi^k(\alpha) = \alpha^{p^k},$$

so we wish to find the minimal k such that $\alpha^{p^k} = \alpha$ for all $\alpha \in F$. Then, for such a k, the polynomial $x^{p^k} - x$ has at least p^n roots in F so it must be that $k \geq n$ since any polymomial has at most its degree number of roots. But we know also that $\varphi^n = \mathrm{id}$, since by the very construction of F as a splitting field, $\alpha^{p^n} = \alpha$ for every $\alpha \in F$. So, $k = n$ i.e. φ of order n in $\mathrm{Aut}\left(F/\mathbb{F}_p\right)$. Hence, we know that $\mathbb{Z}/n\mathbb{Z} \subset \mathrm{Aut}(F/\mathbb{F}^p)$, in particular $\mathrm{Aut}(F/\mathbb{F}^p) \geq n$.

From the general theory, we also know that $\mathrm{Aut}(F/\mathbb{F}^p) \leq [F : \mathbb{F}^p] = n$, and thus we know precisely that $\#\,\mathrm{Aut}(F/\mathbb{F}^p) = n$. Thus, we have in summary the following theorem:

↪**Theorem 3.9**: F is a Galois extension of $\mathbb{F}_p$, whose Galois group is the cyclic group $\mathbb{Z}/n\mathbb{Z}$, with a canonical generator given by the Frobenius automorphism. Concretely,

$$\mathrm{Gal}\left(F/\mathbb{F}_p\right) = \{1, \varphi, \varphi^2, ..., \varphi^{n-1}\}.$$

⊛ **Example 3.7**: Let $q = 8 = 2^3$, then $F = \mathbb{F}_2[x]/\left(x^3 + x + 1\right)$ a (really, *the*) field of cardinality 8. By the theory we've developed here, we also know that F the splitting field of the polynomial $x^8 - x$ over $\mathbb{F}_2$.

§3.8 Generalization of Galois

Here, we aim to extend some of the definitions from previous sections to apply to field extensions of infinite degree.

↪**Definition 3.9** (Normal): An extension E/F is said to be *normal* if every irreducible polynomial in $F[x]$ with a root in E splits into linear factors in $E[x]$.

↪**Theorem 3.10**: If E/F Galois, then E is normal over F.

Proof. In the finite case this was proven Thm. 3.6. ■

We can present a (partial) converse to this statement subject to some technicality.

↪**Definition 3.10** (Separable): An extension E/F is *separable* if every irreducible polynomial with a root in E has no multiple roots in E.

↪**Proposition 3.4**: If $\mathrm{char}(F) = 0$, every extension of F is separable.

Proof. Let $f(x)$ be irreducible in $F[x]$. Suppose $f(x) = (x-r)^e g(x)$ in $E[x]$. Then,

$$f'(x) = e(x-r)^{e-1}g(x) + (x-r)^e g'(x).$$

Then, observe that if $e > 1$, then r still a root of $f'(x)$. In particular, then r a root of $\gcd(f(x), f'(x)) \in F[x]$.

Suppose now $\mathrm{char}(F) = 0$. Write

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \qquad a_i \in F,$$

so

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

Then, $\gcd(f,f')$ must divide f. But f irreducible, so it must be that $\gcd(f,f') = 1$ or f; clearly f cannot divide f' since f' has degree $n-1$ and f has degree n, and thus $\gcd(f,f') = 1$ from which we conclude from our observations above that f cannot have any multiple roots. ■

Remark 3.5: We implicitly used the assumption on the characteristic of the field when taking the derivative; in particular, since $\mathrm{char}(F) = 0$, taking the derivative only reduced the degree by 1, namely, $n \neq 0$. If, say, $\mathrm{char}(F) = p$, then for instance the polynomial of degree p, $f(x) = x^p$, has derivative $f'(x) = px^{p-1} = 0$, of degree 0. In this case, we find $\gcd(f,f') = f$.

↪**Theorem 3.11**: If E/F is finite Galois, then it is separable.

↪**Theorem 3.12**: If E/F is a finite, normal and separable, then E/F is Galois.

Proof. Recall our proof of $\#\mathrm{Aut}(E/F) \leq [E:F]$; the proof of this theorem is identical to that one, but replacing certain inequalities with equalities using the extra hypotheses of normality and separability.

We'll prove by induction the more general statement $\#\mathrm{Hom}_F(K,E) = [K:F]$, where $F \subseteq K \subseteq E$, inducting on the degree of K over F.

Put $n := [K:F]$. If $n = 1$, then $\mathrm{Hom}_F(K,E) = \mathrm{Hom}_F(F,E) = \{\mathrm{id}\}$ so this is trivial.

Suppose the case for $n-1$. Suppose firstly that $K = F(\alpha) = F[x]/p(x)$ where $p(\alpha) = 0$ and $p(x)$ irreducible over F with $\deg(p) = [K:F]$. Then,

$$\mathrm{Hom}_F(K,E) = \mathrm{Hom}_F(F(\alpha),E) = \{\text{roots of } p(x) \text{ in } E\},$$

since any homomorphism is constant on F so determined by α. Namely, we try to construct a ring homomorphism

$$\varphi : F[x]/p(x) \to E$$

or equivalently, $\varphi : F[x] \to E$ such that $p \in \ker(\varphi)$; hence $p(\varphi(x)) = 0$.

By normality and separability, $\#\{\text{roots of } p(x) \text{ in } E\} = \deg(p(x)) = [K:F]$.

Suppose now more generally that $K = F(\alpha_1,\ldots,\alpha_t) = F(\alpha_1,\ldots,\alpha_{t-1})(\alpha_t) =: K_{t-1}(\alpha_t)$, such that $K_{t-1} \subsetneq K$ (else, would be done). By assumption, $[K_{t-1}:F] < [K:F] = n$ so our induction hypothesis applies and we know $\#\mathrm{Hom}_F(K_{t-1},E) = [K_{t-1}:F]$. We need now to show that there are exactly $[K:K_{t-1}]$ extensions of $\varphi_0 : K_{t-1} \to E$ for each $\varphi_0 \in \mathrm{Hom}_F(K_{t-1},E)$.

Let $p(x)$ be the minimal polynomial of α_t over K_{t-1} so $\deg p(x) = [K:K_{t-1}]$ and we can identify $K = K_{t-1}[x]/(p(x))$. If $\varphi|_{K_{t-1}} = \varphi_0$, then since $p(\alpha_t) = 0$,

$$\varphi(p(\alpha_t)) = p^{\varphi_0}(\varphi(\alpha_t)) = 0;$$

for, if

$$p(x) = a_m x^m + \cdots + a_1 x + a_0,$$

with $a_i \in K_{t-1}$, then we denote

$$p^{\varphi_0}(x) = \varphi_0(a_m)x^m + \cdots + \varphi_0(a_1)x + \varphi_0(a_0),$$

i.e. p with the coefficients evaluted on φ_0. Then, $\varphi_0(a_i) \in E$ so $p^{\varphi_0}(x) \in E[x]$. So, $\varphi(\alpha_t)$ a root of $p^{\varphi_0}(x)$ in $E[x]$.

We claim $p^{\varphi_0}(x)$ splits into distinct linear factors in $E[x]$. It suffices to prove that p^{φ_0} has a single root in E, by normality.

We know $p(x)$ has a root in E, namely α_t, so $p(x)|g(x)$ where $g(x)$ the minimal polynomial of α_t over F. By normality and separability, g splits into linear factors over E, and thus $p^{\varphi_0}|g^{\varphi_0}$. But g has coefficients in F so $g^{\varphi_0} = g$ thus $p^{\varphi_0}|g$. so $p^{\varphi_0}(x)$ has exactly $[K : K_{t-1}]$ roots. Thus, we can conclude

$$\begin{aligned}\#\mathrm{Hom}_F(K, E) &= \#\mathrm{Hom}_F(K_{t-1}, E) \times \#\{\text{extensions } \varphi \text{ of } \varphi_0 : K_{t-1} \to F\} \\ &= [K_{t-1} : F][K : K_{t-1}] = [K : F],\end{aligned}$$

so taking $K = E$, we conclude

$$\#\mathrm{Hom}_F(E, E) = \#\mathrm{Aut}(E/F) = [E : F].$$

■

This motivates the following definition generalization, with the benefit that it works for infinite degree extensions.

↪**Definition 3.11** (Galois Extension): An extension E/F is said to be *Galois* if it is normal and separable over F.

In summary we've proven the following:

↪**Theorem 3.13**: If E/F is a finite extension, then TFAE:
1. $\#\mathrm{Aut}(E/F) = [E : F]$;
2. E is normal and separable over F;
3. E is the (a) splitting field of a separable polynomial over F.

↪**Proposition 3.5**: If E/F is a Galois extension and K is any subfield of E containing F, then E/K is also Galois.

Proof. This is immediate from 3. of the previous theorem, and from 2.; if $\alpha \in E$, E/F is normal and separable so there is a polynomial $f(x) \in F[x]$ which is irreducible, splits into distinct linear factors in E, and satisfies $f(\alpha) = 0$. Let $g(x)$ be the minimal polynomial of α over K so $g(x) \in K[x]$, $g(\alpha) = 0$ and g irreducible. So, $f(x) \in K[x]$ as

well so it must be by minimality that $g|f$, in $K[x]$. So, it must be that g splits into distinct linear factors in $E[x]$ since f does. Hence, E/K normal and separable.

Another way of seeing this is the following, using part 1. Let $G = \mathrm{Gal}(E/F)$ and $X = \mathrm{Hom}_F(K, E)$. We saw last time that $\#X = [K : F]$. We have a natural action of G on X; if $\varphi \in X$ and $\sigma \in G$, then define

$$\sigma * \varphi := \sigma \circ \varphi.$$

It turns out that X actually a transitive G-set. Previously, we showed that any $\varphi : K \to E$ extends to a map $\tilde{\varphi} : E \to E$; then if $\varphi_1, \varphi_2 : K \to E$, let $\sigma = \tilde{\varphi}_1 \circ \tilde{\varphi}_2^{-1}$. By the orbit-stabilizer theorem, then, we find that

$$\#X \cdot \#\mathrm{Stab}_G(\mathrm{id} : K \to E) = \#G.$$

We know $\#X = [K : F]$ and $\#G = [E : F]$. Moreover, the elements of G that fix $\mathrm{id} : K \to E$ are precisely the number of elements that fix K, hence $\#\mathrm{Aut}(E/K)$; so, rearranging, we find

$$\#\mathrm{Aut}(E/K) = \frac{[E : F]}{[K : F]},$$

which is equal to $[E : K]$ by multiplicativity. ∎

Remark 3.6: Note that K need not be Galois over F in this setup.

↪**Theorem 3.14**: The map $K \mapsto \mathrm{Gal}(E/K)$ is an injection from $\{\text{subfields } F \subset K \subset E\} \to \{\text{subgroups of } \mathrm{Gal}(E/F)\}$.

Proof. We can show there exists a left-inverse to this map, namely, given $H = \mathrm{Gal}(E/K)$, how can you recover K from H? Let $K = E^H$. ∎

↪**Corollary 3.2**: If E/F is finite Galois, then there are finitely many fields $F \subset K \subset E$.

Proof. $\mathrm{Gal}(E/F)$ is a finite group so has finitely many subgroups. From the previous theorem, then since the map from subfields to subgroupsis injective there are at most $\#\{\text{subgroups}\}$ distinct subfields. ∎

↪**Corollary 3.3**: If E/F is any finite separable extension, then there are finitely many subfields $F \subset K \subset E$.

Proof. If E is separable, E is generated by $\alpha_1, \ldots, \alpha_t$ where the α_j is the root of a separable polynomial $g_j(x) \in F[x]$. Let $\tilde{E}$ be the splitting field of $g_1(x) \cdots g_j(x)$. Then, $\tilde{E}/F$ Galois, and $E \subset \tilde{E}$, hence by the previous corollary there are finitely many fields $F \subset K \subset \tilde{E}$ and thus those K which are also subsets of E is less than this finite number. ∎

Remark 3.7: E/F separable is essential in this corollary. Consider $F = \mathbb{F}_p(u,v)$ where u,v two indeterminates. Let $E = F\left(u^{1/p}, v^{1/p}\right)$. Then, $K_\alpha = F\left(u^{1/p} + \alpha v^{1/p}\right)$ for $\alpha \in F$ are distinct subfields of E containing F.

↪**Theorem 3.15** (Primitive Element Theorem): If E/F is finite and separable, then there exists an $\alpha \in E$ such that $E = F(\alpha) = F[\alpha] \simeq F[x]/(p_\alpha(x))$, where $p_\alpha(x)$ is the minimal polynomial of α in E/F.

Proof. If the ground field F is finite, then the result is clear because then E is also finite, so $E^\times$ is cyclic so finitely generated.

Suppose then F infinite. We know $E = F(\alpha_1, ..., \alpha_n)$; we proceed by induction by n. If $n = 1$ we're done. Suppose $n = 2$, and let $E = F(\alpha, \beta)$. Consider $E_t := F(\alpha + t\beta)$ where $t \in F$, which is an extension of F and a subfield of E. There are infinitely many t's, but by the previous theorem can only be finitely many E_t's. In particular, there must be $t_1, t_2 \in F$ such that $E_{t_1} = E_{t_2}$, namely

$$E_0 := F(\alpha + t_1\beta) = F(\alpha + t_2\beta).$$

Then, $\alpha + t_1\beta, \alpha + t_2\beta \in E_0$, so in particular $(t_1 - t_2)\beta \in E_0$ (by subtracting), and by construction $t_1 \neq t_2$, so we can divide out and conclude $\beta \in E_0$. So, subtracting $t_1 \cdot \beta$ from $\alpha + t_1\beta$, we conclude $\alpha, \beta \in E_0$, so $E_0 \supset E$, but the converse was by construction, so we conclude $E_0 = E$.

Suppose the case for n and let $E = F(\alpha_1, ..., \alpha_{n+1})$. We may rewrite this as $F(\alpha_1, ..., \alpha_n)(\alpha_{n+1})$. Applying the induction hypothesis, we find this equal to $E = F(\beta)(\alpha_{n+1}) = F(\beta, \alpha_{n+1})$, and so applying the $n = 2$ case, we are done. ■

Remark 3.8: The separability assumption is key in the statement. Consider $F = \mathbb{F}_p(u,v)$ and $E = \mathbb{F}_p\left(u^{\frac{1}{p}}, v^{\frac{1}{p}}\right)$, an extension of degree p^2 over F. We claim there is no primitive element. Suppose $\alpha \in E$ is such that $\alpha = R\left(u^{\frac{1}{p}}, v^{\frac{1}{p}}\right) = \frac{f\left(u^{\frac{1}{p}}, v^{\frac{1}{p}}\right)}{g\left(u^{\frac{1}{p}}, v^{\frac{1}{p}}\right)}$. then, $\alpha^p = \frac{f(u,v)}{g(u,v)} \in F$, so $[F(\alpha) : F] = 1$ or p for every $\alpha \in E$. In particular, this means $F(\alpha) \neq E$. Hence, the primitive element theorem doesn't apply; there are infinitely many distinct subfields.

We glossed over the computation of the degree. Note that $u^{\frac{1}{p}}$ satisfies the polynomial $x^p - u$ which is irreducible. $v^{\frac{1}{p}}$ satisfies $x^p - v$, which we claim has no roots in $F\left(u^{\frac{1}{p}}\right)$. If $v = R\left(u^{\frac{1}{p}}, v\right)^p = R(u, v^p)$, which is impossible so v not a pth power in $F\left(u^{1/p}\right)$. So, $\left[F\left(u^{\frac{1}{p}}, v^{\frac{1}{p}}\right) : F\right] = p^2$ by multiplicativity.

We use this theorem to prove the converse of Thm. 3.14.

↪**Proposition 3.6**: $\left[E : E^H\right] = \#H$.

Proof. By the primitive element theorem, $E = E^H(\alpha)$ for some $\alpha \in E$. Consider $H\alpha =$ orbit of α under $H = \{\alpha_1, ..., \alpha_n\}$. We claim $\#H\alpha = \#H$. It must be that $\text{Stab}_H(\alpha) = \{1\}$, since if $g\alpha = \alpha$, $\alpha \in E^H$ which contradicts our construction. From the orbit-stabilizer theorem, we conclude the claim.

Consider then $p(x) = (x - \alpha_1)\cdots(x - \alpha_n) \in E^H[x]$, which is in this space since upon expansion each of the coefficients are fixed under H. $p(\alpha) = 0$; moreover, we claim $p(\alpha)$ is irreducible over E^H. H acts transitively on the roots of the polynomial, by design, so it must be irreducible; if it weren't, then there would be two (or more) orbits of the roots of the polynomial.

Thus, we conclude $\left[E : E^H\right] = \deg(p) = n = \#H$. ■

↪**Corollary 3.4**: $H = \text{Gal}\left(E/E^H\right)$.

In particular, this establishes the following maps:

$$\left\{\begin{array}{c}\text{subfields}\\ F \subset K \subset E\end{array}\right\} \underset{E^H \hookleftarrow H}{\overset{K \mapsto \text{Gal}(E/K)}{\longrightarrow}} \left\{\begin{array}{c}\text{subgroups}\\ H \subset G\end{array}\right\}$$

and in particular,

↪**Theorem 3.16** (Galois Correspondance): These two maps are mutually inverse bijections.

In particular, there is a partial ordering on both of these sets by inclusion, and these maps respect this ordering; namely,

$$F \subset K_1 \subset K_2 \subset E \Rightarrow \text{Gal}(E/K_1) \supset \text{Gal}(E/K_2),$$

and similarly

$$H_1 \subset H_2 \subset G \Rightarrow E^{H_1} \supset E^{H_2}.$$

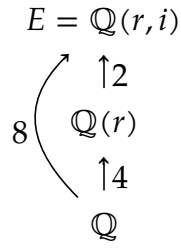
Namely, we say the Galois correspondance is "inclusion reversing".

3.8.1 Computational Example

Let $F = \mathbb{Q}$ and E be the splitting field of $x^4 - 2$. Let $r = \sqrt[4]{2}$ and $E_0 = \mathbb{Q}\left(\sqrt[4]{2}\right)$ so $x^4 - 2 \in E_0[x]$. Moreover, we automatically gain another root, $-\sqrt[4]{2} \in E_0$, so this polynomial factors

$$x^4 - 2 = \left(x - \sqrt[4]{2}\right)\left(x + \sqrt[4]{2}\right)\left(x^2 + \sqrt{2}\right),$$

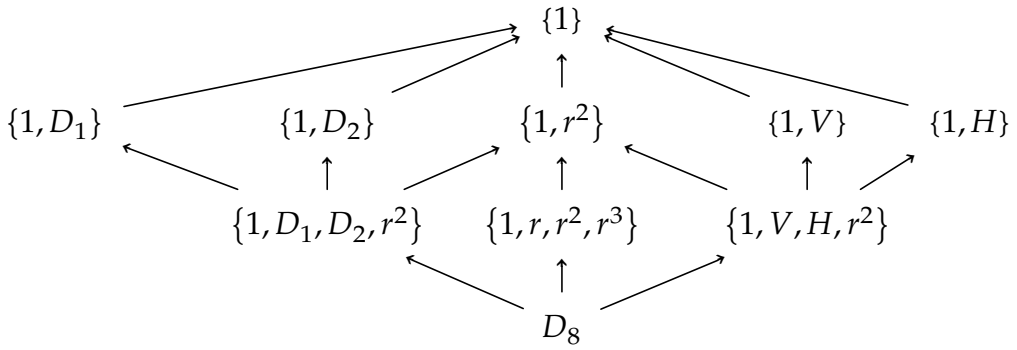
where here we are formally defining $\sqrt{2} = \left(\sqrt[4]{2}\right)^2$; this is no further reducible, so we need to adjoin another element. Let $E = E_0[x]/\left(x^2 + \sqrt{2}\right)$. Note that then $\sqrt{-\sqrt{2}} = i\sqrt[4]{2} = ir$; namely, we can view $E = E_0(ir) = E_0(i)$. So, we have



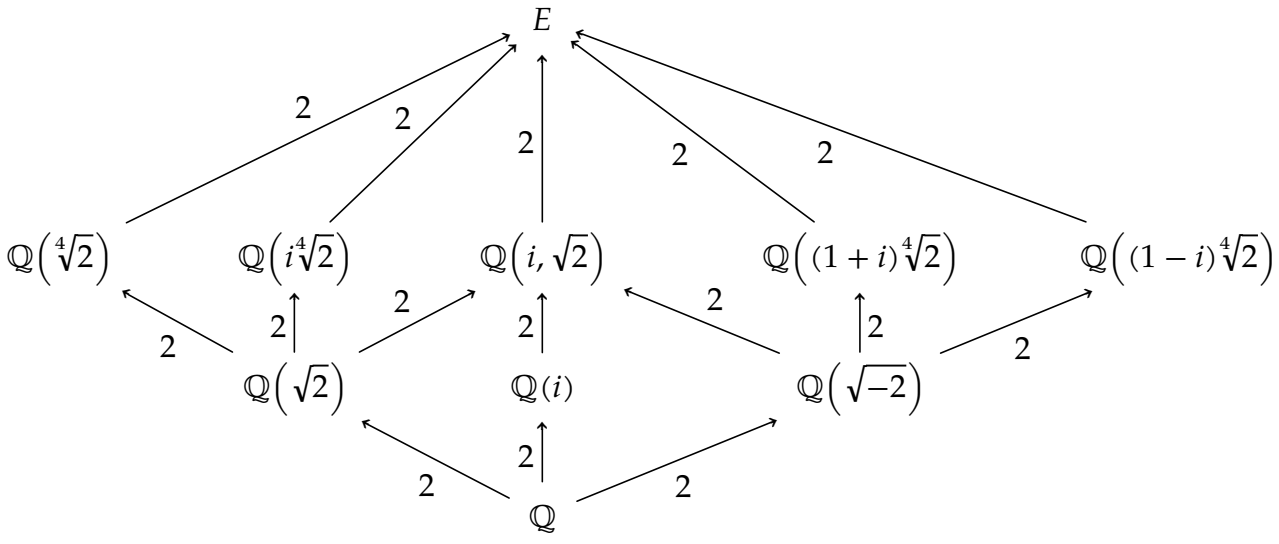
Then, there are 4 roots in E of $x^4 - 2$, namely $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$, and moreover $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ is determined by $(\sigma(r), \sigma(i))$ where $\sigma(r)$ can map to any root and $\sigma(i)$ can map to i or $-i$.

Consider the automorphism $\sigma\left(\sqrt[4]{2}\right) = i\sqrt[4]{2}$, $\sigma(i) = i$. Then, σ acts on the set of roots as a 4-cycle. Another is $\tau\left(\sqrt[4]{2}\right) = \sqrt[4]{2}$, $\tau(i) = -i$. Then, τ swaps $\pm\sqrt[4]{2}$. In particular, σ, τ then generated the entire group, from which we readily see that $\mathrm{Gal}(E/\mathbb{Q}) \simeq D_8$.

Let us relabel $\mathrm{Gal}(E/\mathbb{Q}) = \{1, r, r^2, r^3, D_1, D_2, V, H\}$ in the familiar way, and explore all the possible subfields on E. By the Galois correspondance, we can begin by loooking at the list of all subgroups by inclusion:



This is the so-called "lattice" of subgroups of D_8. For each such subgroup $H \subset D_8$, we can compute E^H and find the following picture;



3.8.2 Complements of Galois Correspondance

↪**Proposition 3.7**: If $\sigma \in \mathrm{Gal}(E/F)$ and $F \subset K \subset E$, $\sigma K = \{\sigma x \mid x \in K\}$ is also a subfield of E/F. Moreover, if H corresponds to K under the Galois correspondance, then $\sigma H \sigma^{-1}$ corresponds to σK under the correspondance.

↪**Theorem 3.17**: Given $F \subset K \subset E$, TFAE:
1. $\sigma K = K$ for every $\sigma \in \mathrm{Gal}(E/F)$;
2. K is Galois over F;
3. $\mathrm{Gal}(E/K)$ is a normal subgroup of $\mathrm{Gal}(E/F)$.

Proof. (1. $\Rightarrow$ 3.) Let $H = \mathrm{Gal}(E/K)$. $\sigma K = K$ for all $\sigma \in G = \mathrm{Gal}(E/F)$ implies, under the Galois correspondance, $\sigma H \sigma^{-1} = H$ for every $\sigma \in G$ so in particular H normal in G.

(1., 3., $\Rightarrow$ 2.) Restriction gives a homomorphism $\eta : \mathrm{Gal}(E/F) \to \mathrm{Aut}(K/F)$. We have that $\ker(\eta) = \{\sigma : \sigma \text{ fixes } K \text{ pointwise}\} = \mathrm{Gal}(E/K)$ hence by the isomorphism theorem $\mathrm{Gal}(E/F)/\mathrm{Gal}(E/K) \hookrightarrow \mathrm{Aut}(K/F)$. Counting the size of the LHS, we readily find

$$\#(\mathrm{Gal}(E/F)/\mathrm{Gal}(E/K)) = \frac{[E:F]}{[E:K]} = [K:F],$$

while $\#\mathrm{Aut}(K/F) \leq [K:F]$, so it must be that equality is achieved i.e. $\#\mathrm{Aut}(K/F) = [K:F]$, and in particular we find the isomorphism

$$\mathrm{Gal}(E/F)/\mathrm{Gal}(E/K) \simeq \mathrm{Gal}(K/F).$$

Other directions left as an exercise. ■

§3.9 Radical Extensions

↪**Definition 3.12** (Radical Extension): An extension E/F is called a *radical extension* if there exists an integer $n \geq 1$ and element $a \in F$ such that $E = F\left[\sqrt[n]{a}\right]$. I.e., assuming $x^n - a$ irreducible in $F[x]$, then $E = F[x]/(x^n - a)$.

↪**Definition 3.13** (Tower of Radicals): A *tower of radical extensions* E/F is a sequence of extensions

$$F = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_n = E,$$

where for each $i = 1, \ldots, n$, E_i is a radical extension of E_{i-1} i.e. $E_i = E_{i-1}\left(\sqrt[n_i]{a_i}\right)$ where $a_i \in E_{i-1}$ and $n_i \geq 1$ an integer.

A classical question in Galois theory is whether every finite extension of $\mathbb{Q}$ is contained in a tower of radical extensions; another way of phrasing this is given a polynomial $f(x) \in \mathbb{Q}[x]$, can its roots be expressed in terms of radicals?

Recall that we said an element $\alpha \in \mathbb{C}$ is *constructible* if it is contained in a tower of quadratic extensions. We saw that not every algebraic number α was constructible by showing that if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, α is not constructible since any tower of quadratic extensions had to have a degree of a power of 2 over $\mathbb{Q}$. We'd like to similarly find some kind of invariant of a general radical extension. However, the degree of such an extension is too crude, without enough structure. Rather, we'll look at properties of the corresponding automorphism group of such extensions.

3.9.1 Automorphism Groups of Radical Extensions

Let $E = F\left(a^{1/n}\right)$ a radical extension. What can we say about $\mathrm{Aut}(E/F)$? In general, it may be trivial (For instance $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$). What conditions do we need to put on F for $F\left(a^{1/n}\right) \subset$ splitting field of $x^n - a$?

Given a single root $a^{1/n}$, then notice that every other root of the form $\zeta^k a^{1/n}$ for $k = 0, \ldots, n-1$ where ζ a primitive nth root of unity. Hence, we have the following:

↪**Theorem 3.18**: Suppose F contains n distinct nth roots of unity, and let $\mu_n(F) \coloneqq \{x \in F^\times \mid x^n = 1\} \simeq \mathbb{Z}/n\mathbb{Z}$ be the group of such elements. Then, $F\left(a^{1/n}\right)$ is Galois with abelian Galois group. Moreover, this group is canonically a subgroup of $\mu_n(F)$.

Proof. If $\sigma \in F\left(a^{1/n}\right)$, then $\sigma\left(a^{1/n}\right)$ must map to some other element which, raising to the n, equals a itself. Then, since F contains n distinct nth roots of unity, then we know moreover that

$$\sigma\left(a^{1/n}\right) = \zeta_\sigma \cdot a^{1/n},$$

where $\zeta_\sigma \in \mu_n(F)$ a root of unity. Moreover, then, this root of unity completely determines the action of σ so we may define a map

$$\eta : \mathrm{Aut}\left(F\left(a^{1/n}\right)\right) \to \mu_n(F), \qquad \sigma \mapsto \zeta_\sigma, \text{ where } \sigma\left(a^{1/n}\right) = \zeta_\sigma \cdot a^{1/n}.$$

Then, one verifies that this is a group homomorphism, and if $\sigma \in \ker(\eta)$, then it must be that $\zeta_\sigma = 1$ so $\sigma = \mathrm{id}_{\mathrm{Aut}}$ hence η an injection. Thus, $\mathrm{Aut}\left(F\left(a^{1/n}\right)\right)$ can be realized as a subgroup of $\mu_n(F)$, which is abstractly isomorphic to $\mathbb{Z}/n\mathbb{Z}$, which is abelian thus $\mathrm{Aut}\left(F\left(a^{1/n}\right)\right)$ itself abelian.

Finally, $F\left(a^{1/n}\right)/F$ can be viewed as the splitting field of $f(x) \coloneqq x^n - a$ over F, since it contains all of the roots of f, and is minimally generated. Thus, the extension is Galois after all.

■

3.9.2 Solvable Groups and the Main Theorem of Galois

↪**Definition 3.14** (Solvable): A finite group G is said to be *solvable* if there is a sequence of subgroups

$$\{1\} \subset G_1 \subset G_2 \subset \cdots \subset G_n = G,$$

such that:
1. $G_{i-1} \lhd G_i$ (G_{i-1} normal in G_i) for each $i = 1, \ldots, n$;
2. G_i/G_{i-1} is abelian for each $i = 1, \ldots, n$.

Remark 3.9: A given G_i need not be normal in the whole G, just G_{i+1}.

⊛ **Example 3.8**:
1. Any abelian group is solvable, $\{1\} \lhd G$
2. S_3 is solvable, $\{1\} \lhd A_3 \lhd S_3$
3. S_4 is solvable, $\{1\} \lhd V := \{(), (12)(34), (13)(24), (14)(23)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \lhd A_4 \lhd S_4$, with
$$S_4/A_4 = \mathbb{Z}/2\mathbb{Z}, \qquad A_4/V = \mathbb{Z}/3\mathbb{Z}.$$
4. S_5 is not solvable; the only normal subgroup is A_5, and A_5 contains no normal subgroups (indeed, then, A_5 also not solvable).

We'll assume throughout that the remainder that $\mathrm{char}(F) = 0$. The main theorem we'd like to get at:

↪**Theorem 3.19**: If E/F is a tower of radical extensions, then it is contained in a Galois extension $\tilde{E}/F$ with solvable Galois group.

Namely, one can "detect" if a given field extension is a tower of radical extensions by checking if it can be embedded in a Galois extension with solvable Galois group.

↪**Proposition 3.8**: If G is a solvable group, then any quotient $\overline{G}$ of G is solvable.

Proof. Write

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

For $\overline{G}$ to be a quotient of G means in particular that there is a surjective map $\eta : G \twoheadrightarrow \overline{G}$. Then, simply take the restriction of η to each subgroup G_i, call this $\eta_i : G_i \twoheadrightarrow \overline{G}_i$, i.e. $\overline{G}_i = \eta(G_i)$. Then, η induces a homomorphism

$$\overline{\eta}_i : G_i/G_{i-1} \to \overline{G}_i/\overline{G}_{i-1}, \qquad aG_{i-1} \mapsto \eta(a)\overline{G}_{i-1}.$$

One readily verifies that this map surjective. Thus, $\overline{G}_i/\overline{G}_{i-1}$ is the image of a surjective map of an abelian group and thus abelian itself.

In particular, we have the following picture:

$$\begin{array}{ccccccccc} \{1\} & \triangleleft & G_1 & \triangleleft & G_2 & \triangleleft \cdots \triangleleft & G_{n-1} & \triangleleft & G_n = G \\ & & \downarrow \eta_1 & & \downarrow \eta_2 & & \downarrow \eta_{n-1} & & \downarrow \eta \\ \{1\} & \triangleleft & \overline{G}_1 & \triangleleft & \overline{G}_2 & \triangleleft \cdots \triangleleft & \overline{G}_{n-1} & \triangleleft & \overline{G}_n \end{array}$$

■

Proof *(Of Thm. 3.19)*. Suppose $F = E_0 \subset E_1 \subset \cdots \subset E_n = E$ where $E_i = E_{i-1}\left(a_i^{1/n}\right)$ for $a_i \in E_{i-1}$. We prove by induction on n.

For $n = 1$, $E = F(\alpha)$ with $\alpha^m = a \in F$. Let $\tilde{E}$ be the splitting field of $x^m - a$, i.e. $\tilde{E} = F(\zeta, \alpha) = F(\zeta)(\alpha)$. Then, we have the tower

$$F \subset F(\zeta) \subset F(\zeta)(\alpha).$$

Then, denoting $\sigma_a \in \mathrm{Gal}(F(\zeta)/F)$ which maps $\zeta \mapsto \zeta^a$ (for $a \in (\mathbb{Z}/m\mathbb{Z})^\times$), one readily verifies $\sigma_a \circ \sigma_b = \sigma_{ab}$ so in particular we obtain an injection

$$\mathrm{Gal}(F(\zeta)/F) \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times.$$

This gives in particular $\mathrm{Gal}(F(\zeta)/F)$ abelian. Then, since $\zeta \in F(\zeta)$, it follows that $\mathrm{Gal}(F(\zeta, \alpha)/F(\zeta))$ is also abelian, being a subgroup of $\mathbb{Z}/m\mathbb{Z}$ (more concretely, as the group of mth roots of unity) as well. Finally, $\mathrm{Gal}(F(\alpha, \zeta)/F)$ is abelian too since it is a splitting field.

Let $G_1 = \mathrm{Gal}(F(\zeta, \alpha)/F(\zeta))$ and $G = \mathrm{Gal}(F(\zeta, \alpha)/F)$. We claim G_1 normal in G. Indeed,

$$F(\zeta, \alpha)^{G_1} = F(\zeta)$$

is Galois over F, and since under the Galois correspondance

$$G \leftrightarrow F, \qquad G_1 \leftrightarrow F(\zeta), \qquad 1 \leftrightarrow F(\zeta, \alpha),$$

and since $F(\zeta)/F$ is Galois, the corresponding Galois group G_1 is normal in G, and so again by the correspondance $G/G_1 = \mathrm{Gal}(F(\zeta)/F) \subset (\mathbb{Z}m\mathbb{Z})^\times$. Thus, $F(\alpha) \subset F(\alpha, \zeta)$ which is Galois with solvable Galois group, thus proving the base case.

Suppose the claim for $n - 1$. We have

$$\begin{array}{ccc} E_{n-1} & \subset & E_n = E_{n-1}(\beta) \\ \cap & & \\ \tilde{E}_{n-1} & & \end{array},$$

where $\beta^m = b \in E_{n-1}$. By the induction hypothesis, $\tilde{E}_{n-1}/F$ is solvable.

Let $\{b_1, \ldots, b_t\}$ be the orbit of b under $\mathrm{Gal}\left(\tilde{E}_{n-1}/F\right)$ and let

$$g(x) := (x^m - b_1)(x^m - b_2)\cdots(x^m - b_t).$$

Then, $g \in F[x]$, since it's coefficients are fixed under $\mathrm{Gal}\left(\tilde{E}_{n-1}/F\right)$. Let $\tilde{E}_n$ be the splitting field of $g(x)$ over F. In particular, we can write

$$\tilde{E}_n = \tilde{E}_{n-1}\left(\sqrt[m]{b_1}, \sqrt[m]{b_2}, \ldots, \sqrt[m]{b_t}, \zeta\right),$$

where ζ an mth root of unity. Then, we can view this as the following tower of extensions:

$$\begin{array}{c} \tilde{E}_{n-1}\left(\zeta, \sqrt[m]{b_1}, \sqrt[m]{b_2}, \ldots, \sqrt[m]{b_t}\right) \\ \uparrow H \\ \tilde{E}_{n-1}(\zeta) \\ \uparrow \subset (\mathbb{Z}/m\mathbb{Z})^\times \\ \tilde{E}_{n-1} \end{array}$$

Then, we find that similar to the base case, $\mathrm{Gal}\left(\tilde{E}_{n-1}(\zeta)/\tilde{E}_{n-1}\right) \subset (\mathbb{Z}/m\mathbb{Z})^\times$, and if we put $H = \mathrm{Gal}\left(\tilde{E}_n/\tilde{E}_{n-1}\right)$, automorphisms here are determined by how they act on an t tuple of mth roots, and thus

$$H \subseteq \mathbb{Z}/m\mathbb{Z} \times \cdots \times \mathbb{Z}/m\mathbb{Z},$$

so in particular H abelian and $H \lhd G := \mathrm{Gal}\left(\tilde{E}_n/\tilde{E}_{n-1}\right)$, and so that $G/H \subset (\mathbb{Z}/m\mathbb{Z})^\times$. Thus, we find that G is solvable and normal in $\mathrm{Gal}\left(\tilde{E}_n/F\right)$ and so $\mathrm{Gal}\left(\tilde{E}_n/F\right)/G$ is solvable thus $\mathrm{Gal}\left(\tilde{E}_n/F\right)$ is solvable.

■

↪**Theorem 3.20** (Main Theorem of Galois): If $f(x) \in F[x]$ is solvable by radicals, then $\mathrm{Gal}(f)$ is a solvable group (where $\mathrm{char}(F) = 0$).

Proof. If $f(x)$ is solvable, then E the splitting field of F is contained in a tower of radical extensions. Therefore, E is contained in a solvable extension of F, say $\tilde{E}$;

$$F \subset E \subset \tilde{E}.$$

If $G = \mathrm{Gal}(E/F)$, then, G is a quotient of $\tilde{E}/F$ and thus G is solvable. ■

↪**Theorem 3.21**: If $f(x)$ is a quintic polynomial and $\mathrm{Gal}(f) = S_5$, then $f(x)$ is not solvable by radicals.

To show this theorem not vacuous, we first show that there exists such a polynomial, with $F = \mathbb{Q}$.

↪**Proposition 3.9**: Let G be a transitive subgroup of S_5 containing a transposition. Then, $G = S_5$.

Proof. G transitive implies $5|\#G$ by orbit-stabilizer so we can assume WLOG that $\sigma = (12345) \in G$ and $\tau = (12) \in G$. Conjugating τ by $\sigma, \sigma^2, \sigma^3, \sigma^4$, we further find $(23), (34), (45), (51) \in G$. Further conjugating τ by (23) we find $(13) \in G$. We can then conjugate this element by σ, and repeat, and ultimately find al the transpositions are in G. Since such elements generate S_5, we conclude $G = S_5$. ■

↪**Proposition 3.10**: Let $f(x)$ be a polynomial of degree 5 satisfying:
1. $f(x)$ is irreducible over $\mathbb{Q}$;
2. $f(x)$ has exactly three real roots.

Then, $\mathrm{Gal}(f) = S_5$.

Proof. Let $r_1, ..., r_5$ the roots of f and so $E = \mathbb{Q}(r_1, ..., r_5)$ the splitting field of f. We want to show that there exists an automorphism of order 2 that acts on the roots as a transposition, since then by the previous proposition we'd be done since condition 1. ensures $\mathrm{Gal}(E/\mathbb{Q})$ is transitive acting on the roots.

We can embed $E \subset \mathbb{C}/\mathbb{R}$. The only automorphisms of $\mathbb{C}/\mathbb{R}$ are the identity and complex conjugation. Then, restricting complex conjugation to $E/\mathbb{Q}$, we find a automorphism of order 2, and since 3 of the roots are real, this conjugation will leave them fixed, hence we are indeed done. ■

We prove now a converse of Thm. 3.20:

↪**Theorem 3.22**: Every solvable extension of F is constructible by radicals.

Proof. We remark first:
1. It is enough to show this for abelian E/F, since E solvable so $F \subset E_1 \subset \cdots \subset E_n = E$, and each quotient abelian. So if we can prove for each "subextension", we're done.
2. We can assume F contains the nth roots of unity where $n = [E : F]$ by just adjoining them if not.

Now, we can view E as an F-linear representation of $G = \mathrm{Gal}(E/F)$. Since G abelian, we know each of its irreducible representations are one-dimensional. We can write then

$$E = \bigoplus_{\chi \in \hat{G}} E[\chi],$$

$$\hat{G} = \mathrm{Hom}(G, F^*), \qquad E[\chi] = \{v \in E \mid \sigma v = \chi(\sigma) v \ \forall\, \sigma \in G\},$$

since we can identify one dimensional representations with maps into $F^\times$ (where we are crucially using that F contains enough roots of unity).

We claim $\dim_F E[\chi] \leq 1$. Suppose $v \in E[\chi]$ and $v \neq 0$, and let $w \in E[\chi]$. We claim they differ by a scalar. Consider $\frac{w}{v} \in E$. For any $\sigma \in G$

$$\sigma\Big(\frac{w}{v}\Big) = \frac{\sigma(w)}{\sigma(v)} = \frac{\chi(\sigma)w}{\chi(\sigma)v} = \frac{w}{v},$$

hence $\frac{w}{v} \in E^G = F$ so $w = \lambda v$ for some $\lambda \in F$. It follows that $E[\chi] = F \cdot v$, so $E[\chi]$ has dimension (at most) 1.

Let us compare now dimension on each side; on the one hand,

$$\dim_F E = [E : F] = \#G = n,$$

while

$$\dim_F \bigoplus_\chi E[\chi] = \sum_{i=1}^{n} \dim_F E[\chi] \leq \#\hat{G} = n,$$

so equality must actually be attained, and in particular each $E[\chi]$ must have dimension one (i.e. every irreducible component 'appears' precisely once). Thus, we find that E is isomorphic to the regular representation of G, namely $F[G]$, as a representation of G.

Remark 3.10: This is in fact always true for abelian extensions, for general, not necessarily abelian G.

For each $\chi \in \hat{G}$, let $y_\chi \in E[\chi]$ be a basis (generator), so

$$E = F\big(y_\chi : \chi \in \hat{G}\big).$$

For any $\sigma \in G$, then

$$\sigma\big(y_\chi^n\big) = \sigma\big(y_\chi\big)^n = \big(\chi(\sigma) \cdot y_\chi\big)^n = \chi(\sigma)^n \cdot y_\chi^n = y_\chi^n,$$

since $\chi(\sigma)$ some nth root of unity, since G abelian. So, $y_\chi^n =: a_\chi \in E^G = F$, and thus $y_\chi = a_\chi^{\frac{1}{n}}$ and in particular

$$E = F\big(a_\chi^{1/n} : \chi \in \hat{G}\big),$$

completing the proof. ∎

3.9.3 Solution to the Cubic, Revisted

Recall we can write any cubic with distinct roots (over $\mathbb{Q}$) as $x^3 + px + q = (x - r_1)(x - r_2)(x - r_3)$ with $G \subset S_3$ the Galois group of $E = \mathbb{Q}(r_1, r_2, r_3)$, which acts transitively on the roots so either $\mathbb{Z}/3\mathbb{Z}$ or S_3. We have

$$\mathbb{Q} \text{ —}^2 K \text{ —}^{\mathbb{Z}/3\mathbb{Z}} E.$$

Let $\sigma = (r_1 r_2 r_2)$. We want to diagonalize σ. It should have eigenvalues $1, \zeta$ or ζ^2 where ζ a primitive 3rd root of unity. Consider $v_1 = r_1 + \zeta r_2 + \zeta^2 r_3$, then $\sigma v_1 = \zeta^2 v_1$ and $v_2 = r_1 + \zeta^2 r_2 + \zeta r_3$, then $\sigma v_2 = \zeta v_2$. So, these two vectors are eigenvectors. There are a plethora of eigenvectors with eigenvalue 1, such as the symmetric functions on r_1, r_2, r_3. Then, we find in particular that

$$v_1^3, v_2^3 \in E^\sigma(\zeta) = K(\zeta),$$

and so

$$r_1 + \zeta r_2 + \zeta^2 r_3 = \sqrt[3]{A}, \qquad r_1 + \zeta^2 r_2 + \zeta r_3 = \sqrt[3]{B},$$

where $A, B \in K(\zeta)$. We don't like ζ here; if we add these two, we find

$$2r_1 - r_2 - r_3 = \sqrt[3]{A} + \sqrt[3]{B}.$$

In particular, recall that in our "depleted cubic", the sum of the roots equals zero, so this simplifies

$$3r_1 = \sqrt[3]{A} + \sqrt[3]{B} \Rightarrow r_1 = \sqrt[3]{\frac{A}{27}} + \sqrt[3]{\frac{B}{27}}.$$

Similarly, we can study the quartic equation. We have the chain of normal subgroups

$$S_4 \rhd A_4 \rhd V (\rhd \{1, \tau\} \rhd) \rhd 1,$$

namely S_4 solvable. Let $f(x)$ be quartic and E the splitting field of f, assuming $\mathrm{Gal}(f) = S_4$. By this chain of normal subgroups above and the Galois correspondance, we should find a corresponding sequence of subfields fixed by the corresponding subgroups

$$\mathbb{Q} \subset K \subset L \subset L' \subset E.$$

By looking at the degrees, the first would append a square root, the second a cube root, and the last two another two square roots.

Consider $V \lhd S_4$. We know L Galois over $\mathbb{Q}$, and so $\mathrm{Gal}(L/\mathbb{Q}) = S_4/V = S_3$. This seems to imply we can reduce our quartic to a cubic! Suppose f factors

$$f(x) = (x - r_1)(x - r_2)(x - r_3)(x - r_4).$$

We seek a polynomial $g(x) \in \mathbb{Q}[x]$ such that the splitting field of g is L. In particular, we wish to find an element in E that is fixed under V but not globally fixed by S_4. Consider $r := r_1 r_2 + r_3 r_4$. It is fixed under V, but under the action of S_4 can map to $r_1 r_3 + r_2 r_4$ and $r_1 r_4 + r_2 r_3$, so in particular r has 3 Galois conjugates. The minimal polynomial of r (namely, the "cubic resolvent") can be written

$$g(x) = (x - (r_1 r_2 + r_3 r_4))(x - (r_1 r_3 + r_2 r_4))(x - (r_1 r_4 + r_2 r_3)) \in E^{S_4}[x] = \mathbb{Q}[x].$$

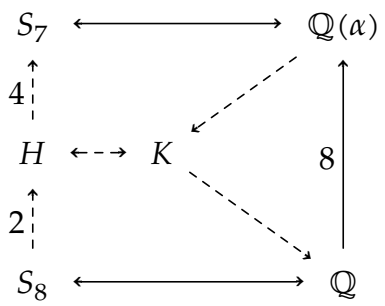
Let us assume $f(x) = x^4 + ax^2 + bx + c$ where $a, b, c \in \mathbb{Q}$. We wish then to find the coefficients of g in terms of a, b, c.

$$g(x) = x^3 - (r_1 r_2 + r_3 r_4 + r_1 r_3 + r_2 r_4 + r_1 r_4 + r_2 r_3)x^2 + \cdots$$

The quadratic term is the pairwise product, which we see to be equal to a (namely the second symmetric function) so $g(x) = x^3 - ax^2 + \cdots$. The remaining terms can be found with a little more work, but ultimately are polynomials in a, b, c.

3.9.4 Back to Constructible Numbers

Recall that we showed that if a number α is constructible by ruler and compass, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^t$ for some $t \geq 0$. Let $f(x)$ be any irreducible polymomial of degree 8 over $\mathbb{Q}$. Assume that $f(x)$ has a Galois group S_8. Then, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$, but we claim α not solvable. Under the Galois correspondance, we have the following setup then:



In particular, if $\mathbb{Q}(\alpha)$ were constructible, then we should be able to "insert" an intermediary field K such that it has a Galois group H such that $S_8 \supset H \supset S_7$. But this is not possible:

↪**Proposition 3.11**: For $n \geq 4$, S_{n-1} is a maximal subgroup of S_n.

Proof. If such a subgroup existed, $H \subset S_n$, then S_n acts on S_n/H which implies a map $S_n \twoheadrightarrow S_t$ for some $t < n$. ■

This leads to an improved theorem:

↪**Theorem 3.23**: α is constructible by ruler and compass if and only if $\mathbb{Q}(\alpha)$ is contained in a Galois $E/\mathbb{Q}$ with $\#\mathrm{Gal}(E/\mathbb{Q}) = 2^t$.

Indeed, this suggests the following theorem:

↪**Theorem 3.24**: Every group of cardinality p^t is solvable where p prime.

Indeed, such a group must have nontrivial center $Z(G)$. From here, one can proceed by induction on $G/Z(G)$, which will now be a group of a smaller prime power.

3.9.5 The Fundamental Theorem of Algebra

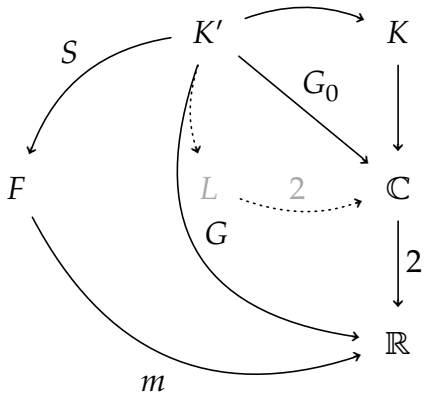
We apply some of the ideas from before to proving

↪**Theorem 3.25**: $\mathbb{C}$ is algebraically closed.

We'll assume the following facts:

1. Every polynomial of odd degree in $\mathbb{R}[x]$ has a root in $\mathbb{R}$ (by intermediate value theorem); thus every odd degree extension of $\mathbb{R}$ is *trivial*.
2. Every quadratic equation in $\mathbb{C}[x]$ has a root in $\mathbb{C}$ (from the quadratic formula).

Proof. Let K be a finite extension of $\mathbb{C}$ and K' the Galois closure of K over $\mathbb{R}$:



Let G be the Galois group of K' over $\mathbb{R}$. Then, $\#G = 2^t m$ for some m odd, so by the Sylow theorems, G has a subgroup of cardinality 2^t, call it S, and let $F = (K')^S$ be the corresponding field extension over $\mathbb{R}$. Then, $[F : \mathbb{R}] = m$, which is odd. By the previous remarks, $F = \mathbb{R}$, and thus S must equal G and in particular $\#G = 2^t$.

Let $G_0 := \mathrm{Gal}(K'/\mathbb{C})$, then $\#G_0 = 2^{t-1}$. If G_0 is nontrivial, then it contains a subgroup G_{00} if index 2 in G_0. Let $L = (K')^{G_{00}}$ be the corresponding field. Then, L is a quadratic extension of $\mathbb{C}$, which doesn't exist and thus we have a contradiction, i.e. $L = \mathbb{C}$. Thus, it must be that G_0 is trivial, and hence $K' = \mathbb{C}$. ■

3.9.6 Systematic Computation of Galois Groups

Consider a polynomial f in variables $x_1, ..., x_r$ over $\mathbb{Q}$, where $G := \mathrm{Gal}(f) \subseteq S_n$. Define the *resolvent* of f as

$$R(x_1, ..., x_n) := \prod_{\sigma \in S_n} (r_1 x_{\delta 1} + r_2 x_{\delta 2} + \cdots + r_n x_{\delta n}).$$

This polynomial lives in $E^G[x_1, ..., x_n] = \mathbb{Q}[x_1, ..., x_n]$. This polynomial factors, in $\mathbb{Q}[x_1, ..., x_n]$, into

$$R(x_1, ..., x_n) = R_1 R_2 ... R_t.$$

There is a natural action of S_n on these factors.

↪**Theorem 3.26**: $G = \mathrm{Stab}_{S_n}(R_1)$.

Proof. We may write

$$R(x_1, ..., x_n) = \prod_{\Sigma \in S_n/G} \left(\prod_{\sigma \in \Sigma} \left(\underbrace{r_1 x_{\sigma 1} + \cdots r_n x_{\sigma n}}_{\text{irreducible over } \mathbb{Q}} \right) \right),$$

and the stabilizer of R_1 is G. ■

There are more efficient ways, particularly over finite field. Suppose $f(x) \in \mathbb{F}_p[x]$. Then, recall that $x^p - x$ has as factors every element in $\mathbb{F}_p$. Then,

$$\gcd(f(x), x^p - x) = \prod_{f(r)=0} (x - r).$$

This still isn't necessarily easy, but one can begin by rewriting $x^p - x \bmod f(x)$; one begins by writing $x^p = x\left(x^{\frac{p-1}{2}}\right)^2 \bmod f(x)$. Then, one proceeds by computing via the Euclidean algorithm, which will be on the order of about $\log(p)$ (?).

Given some $f \in \mathbb{Q}[x]$, then, one can, through manipulation, place $f \in \mathbb{Z}[x]$ (by clearing denominators, etc). Then, one can consider $f \bmod p \in \mathbb{Z}/p\mathbb{Z}[x]$ for various p to study its roots using the above algorithm.

3.9.7 "The Converse Problem of Galois Theory"

One natural converse to our work above is whether given a group G, does there exist an extension $E/\mathbb{Q}$ with $\mathrm{Gal}(E/\mathbb{Q}) = G$? This is still very much open, but the following holds:

↪**Theorem 3.27**: For any finite group G, there exists E/F with $[F : \mathbb{Q}] < \infty$ with $\mathrm{Gal}(E/F) = G$.

The idea is to:

1. Embed $G \subset S_n$ (Lagrange), and suppose wlog n prime.
2. We see $E/\mathbb{Q}$ is an extension with Galois group S_n.
3. Let $F = E^G$, then by Galois correspondance $\mathrm{Gal}(E/F) = G$.

§4 Final Exercises

↪**Proposition 4.1**: Let $f(x)$ be an irreducible polynomial over F and assume that $f(x)/(x-r)$ remains irreducible over $F(r)$ where r is a root of $f(x)$. Show that the Galois group of $f(x)$ over F acts doubly transitively on the set of roots of f.

Proof. Denote by E the splitting field of f over F. Since $f(x)/(x-r)$ remains irreducible in $F(r)$, E is also the splitting field of $f(x)/(x-r)$ over $F(r)$. Let $r_1 \neq r_3, r_2 \neq r_4$ be four roots of $f(x)$ in E/F. Since $\mathrm{Gal}(f(x)/(x-r))$ acts transitively on the set of roots minus r of f, pick $\varphi \in \mathrm{Gal}(f(x)/(x-r))$ ■

↪**Proposition 4.2**: Suppose that $f(x)$ is a polynomial of degree n over $F = \mathbb{Q}$ satisfying the hypotheses in Q1, and assume that $f(x)$ has exactly $n-2$ real roots. Show that the Galois group of $f(x)$ is equal to S_n.

Proof. The existence of a pair of complex conjugate roots means there is a transposition in $G = \mathrm{Gal}(f)$. G then a doubly-transitive subgroup of S_n containing a transposition, which we assume wlog is $(r_1 r_2)$ acting on the set of roots of f. For any two roots $r_3 \neq r_4$, pick $\varphi \in G$ such that $\varphi(r_3) = r_1, \varphi(r_4) = r_2$, appealing to double-transitivity. Then,

$$\left(\varphi^{-1}\circ(r_1r_2)\circ\varphi\right)(r_k)=\begin{cases}r_4 \text{ if } k=3\\ r_3 \text{ if } k=4,\\ r_k \text{ o.w.}\end{cases}$$

hence $\varphi^{-1}\circ(r_1r_2)\circ\varphi=(r_3r_4)$. In this manner, we can generate every transposition in G, hence since such elements generate S_n, we conclude $G=S_n$. ■

↪**Proposition 4.3**: Let G be a finite group. Show that there exists fields $E\supset F$ for which $\mathrm{Gal}(E/F)$ is isomorphic to G.

Proof. Let n be such that $G\subset S_n$, appealing to Lagrange; assume wlog n is prime. Then, let $f(x)\in\mathbb{Q}[x]$ be an irreducible polynomial with exactly 2 complex roots and $n-2$ real roots. Let E be the splitting field of $f(x)$ over $\mathbb{Q}$. Then, we claim $H:=\mathrm{Gal}(E/\mathbb{Q})=S_n$.

First, H acts transitively on the set of n roots of $f(x)$ so $n|\#H$. By Sylow, there is a copy of $\mathbb{Z}/n\mathbb{Z}\subset H$, hence an n-cycle, in H, WLOG $(12\ldots n)$.

Then, since there is a complex conjugate pair of roots of f, complex conjugation i.e. a transposition exists in H, call it (ab).

Since n prime, (ab), $(12\ldots n)$ generate S_n thus $H=S_n$.

Finally, let $F=E^G$. By the Galois correspondance, $\mathrm{Gal}(E/F)=G$. ■

↪**Proposition 4.4**: Let p be a prime and let $f(x)$ be a polynomial of degree $p+1$ over a field F, whose galois group is isomorphic to the group $\mathrm{PGL}_2\left(\mathbb{F}_p\right)$. Show that the splitting field of $f(x)$ over F is generated over F by any three of its roots r_1,r_2,r_3. Show that $f(x)/(x-r_1)$ is irreducible over $F(r_1)$ and $f(x)/(x-r_1)(x-r_2)$ is irreducible over $F(r_1,r_2)$.

↪**Proposition 4.5**: List all the subfields of the field $\mathbb{Q}(\zeta)$ generated by a primitive 8th root of unity.

Proof. Let $G=\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ (which is galois being the splitting field of x^4+1). There are 4 primitive 8th roots of unity, $\pm\frac{\sqrt{2}}{2}\pm\frac{\sqrt{2}}{2}i$, just label $\zeta=\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i$. Any homomorphism $\varphi\in G$ is determined by φ and moreover must map φ to another primitive 8th root of unity, so one of either $\zeta,-\zeta,\overline{\zeta},-\overline{\zeta}$; viewing φ as a permutation on $\left\{\zeta,-\zeta,\overline{\zeta},-\overline{\zeta}\right\}$, we readily find:

$$\begin{array}{ll}\zeta\mapsto\zeta & ()\\ \zeta\mapsto-\zeta & (12)(34)\\ \zeta\mapsto\overline{\zeta} & (13)(24)\\ \zeta\mapsto-\overline{\zeta} & (14)(23)\end{array}$$

From here we see $G \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$, which has four subgroups, the identity and three copies of $\mathbb{Z}/2$:

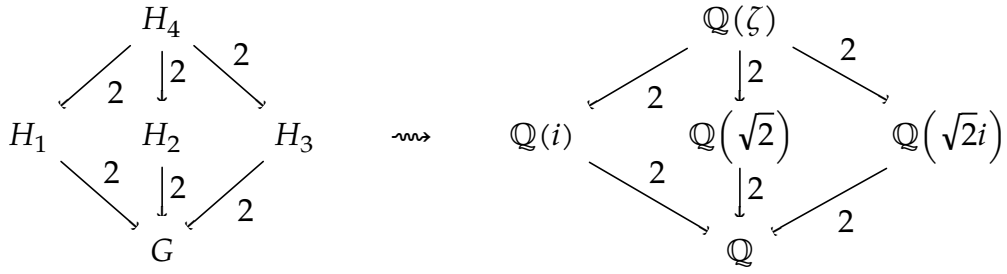
$$H_1 := \langle (12)(34) \rangle \rightsquigarrow \text{fixes } i \qquad \left(\text{since } i = \zeta^2 \mapsto (-\zeta)^2 = \zeta^2 = i\right)$$

$$H_2 := \langle (13)(24) \rangle \rightsquigarrow \text{fixes } \zeta + \overline{\zeta} = \sqrt{2}$$

$$H_3 := \langle (14)(23) \rangle \rightsquigarrow \text{fixes } \sqrt{2}i \qquad \left(\text{since } \sqrt{2}i = \zeta - \overline{\zeta} \mapsto -\overline{\zeta} + \zeta = \sqrt{2}i\right)$$

$$H_4 := 1 \rightsquigarrow \text{fixes } \mathbb{Q}$$

Appealing to the galois correspondance, we find the following subfield correspondance:



In summary, the five distinct subfields of $\mathbb{Q}(\zeta)$ are itself, $\mathbb{Q}(i)$, $\mathbb{Q}\left(\sqrt{2}\right)$, $\mathbb{Q}\left(\sqrt{2}i\right)$, $\mathbb{Q}$. Note that there are no further subfields of $\mathbb{Q}$ since $\mathbb{Q}$ generated by 1. ■

↪**Proposition 4.6**: Show that the extension $\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ is Galois over $\mathbb{Q}$, and compute its Galois group.

Proof.

Let $f(x) = \left(x^2-2\right)^2 - 2 = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$. Letting $r_1 := \sqrt{2+\sqrt{2}}$, $r_2 := -r_1$, $r_3 := \sqrt{2-\sqrt{2}}$ and $r_4 := -r_3$ enumerates the roots of f. Then, certainly $\mathbb{Q}(r_1, r_3)/\mathbb{Q}$ the splitting field of f and $\mathbb{Q}(r_1) \subset \mathbb{Q}(r_1, r_3)$. We claim this is an equality, namely that $r_3 \in \mathbb{Q}(r_1)$. Indeed, notice that

$$r_1 r_3 = \sqrt{\left(2+\sqrt{2}\right)\left(2-\sqrt{2}\right)} = \sqrt{2},$$

and $\sqrt{2} \in \mathbb{Q}(r_1)$ since $r_1^2 - 2 = \sqrt{2}$. Thus, $r_3 = \sqrt{2} \cdot r_1^{-1} \in \mathbb{Q}(r_1)$. Thus, $\mathbb{Q}(r_1) = \mathbb{Q}[x]/(f(x))$ so is Galois over $\mathbb{Q}$.

Moreover, since f of degree 4, $[\mathbb{Q}(r_1) : \mathbb{Q}] = 4$, so we have two options for the Galois group. Consider the map $r_1 \mapsto r_3$. One verifies that this is a 4-cycle acting on the roots of f, from which it follows that $\mathrm{Gal}(\mathbb{Q}(r_1)/\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$.

Note that, more generally, $\mathbb{Q}\left(\sqrt{d}\right)$ a quadratic extension of $\mathbb{Q}$ and we adjoin an additional elements $\sqrt{a+b\sqrt{d}}, \sqrt{a-b\sqrt{d}}$, that we have the relation $\sqrt{a+b\sqrt{d}} \cdot \sqrt{a-b\sqrt{d}} = \sqrt{a^2-b^2d}$ so

if in particular $a^2 - b^2 d$ a perfect square in $\mathbb{Q}$ or $\mathbb{Q}\left(\sqrt{d}\right)$, then we are in a similar situation to the above.

■

↪**Proposition 4.7**: Show that the symmetric group S_{12} contains subgroups of cardinality 31104 and 82994 (Hint: $31104 = (3!)^4 \cdot 4!$ and $82294 = (4!)^3 \cdot 3!$). Explain how you might try to go about constructing degree 12 polynomials with those Galois groups.

Proof. $\#S_{12} = 12! =$ ■