1 Background Material

First we will review some basic information about p-adic fields. This is a modified version of the corresponding section from my Number Theory II notes. Second we will review some basics of representation theory, with a focus on representations of finite groups.

There are many places to read about both of these topics. For example, Svetlana Katok's book *p-adic Analysis Compared with Real* for the p-adic numbers. For representation theory of finite groups, the classic is Serre's *Linear Representations of Finite Groups*. Other recommendations are the first part of Fulton and Harris's *Representation Theory*, and James and Liebeck's *Representations and Characters of Groups*. Fulton and Harris also includes the representation theory of $\mathrm{GL}_2(\mathbb{F}_p)$, which is an illuminating analogue to what we will study.

1.1 p-adic fields

If R is an integral domain, a map $|\cdot| : R \to \mathbb{R}$ which satisfies

(i) $|x| \geq 0$ with equality if and only if $x = 0$,
(ii) $|xy| = |x||y|$, and
(iii) $|x + y| \leq| x| + |y|$

is called an **absolute value** on R. Two absolute values $|\cdot|_1$ and $|\cdot|_2$ are equivalent on R if $|\cdot|_2 = |\cdot|_1^c$ for some $c > 0$. If we have an absolute value $|\cdot|$ on R, by (ii), we know $|1 \cdot 1| = |1| = 1$. Similarly, we know $|-1|^2 = |1| = 1$, and therefore $|-x| = |x|$ for all $x \in R$.

Now a absolute value $|\cdot|$ on R makes R into a metric space with distance $d(x, y) = |x-y|$. (The fact $|-x| = |x|$ guarantees $|y-x| = |x-y|$ so the metric is symmetric, and (iii) gives the triangle inequality.) Recall that any metric space is naturally embued with a topology. Namely, a basis of open (resp. closed) neighborhoods around any point $x \in R$ is given by the set of open (resp. closed) balls $B_r(x) = \{y \in R : d(x, y) = |x - y| < r\}$ (resp. $\overline{B}_r(x) = \{y \in R : d(x, y) = |x - y| \leq r\}$) centered at x with radius $r \in \mathbb{R}$.

Ostrowski's Theorem says, that up to equivalence, every absolute value on $\mathbb{Q}$ is of one of the following types:

$|\cdot|_0$, the trivial absolute value, which is 1 on any non-zero element
$|\cdot|_\infty$, the usual absolute value on $\mathbb{R}$
$|\cdot|_p$, the **p-adic absolute value**, defined below, for any prime p.

Here the p-adic absolute value defined on $\mathbb{Q}$ is given by

$$|x| = p^{-n}$$

where $x = p^n \frac{a}{b}$ with $p \nmid a, b$. (Note any $x \in \mathbb{Q}$ can be uniquely written as $x = p^n \frac{a}{b}$ where $p \nmid a, b$ and $\frac{a}{b}$ is reduced.)

In particular, if $x \in \mathbb{Z}$ is relatively prime to p, we have $|x| = 1$. More generally, if $x \in \mathbb{Z}$, $|x| = p^{-n}$ where n is the number of times p divides x.

Note any integer $x \in \mathbb{Z}$ satisfies $|x|_p \leq 1$, and $|x|_p$ will be close to 0 if x is divisible by a high power of p. So two integers $x, y \in \mathbb{Z}$ will be close with respect to the p-adic metric if $p^n | x - y$ for a large n, i.e., if $x \equiv y \bmod p^n$ for large n.

Example 1.1.1. *Suppose $p = 2$. Then*

$$|1|_2 = 1,\ \ |2|_2 = \frac{1}{2},\ \ |3|_2 = 1,\ \ |4|_2 = \frac{1}{4},\ \ |5|_2 = 1,\ \ |6|_2 = \frac{1}{2}, \ldots$$

$$|\frac{3}{4}|_2 = 4,\ \ |\frac{12}{17}|_2 = \frac{1}{4},\ \ |\frac{57}{36}|_2 = 4.$$

With respect to $|\cdot|_2$, the closed ball $\overline{B}_{1/2}(0)$ of radius $\frac{1}{2}$ about 0 is simply all rationals (in reduced form) with even numerator. Similarly $\overline{B}_{1/4}(0)$ of radius $\frac{1}{4}$ about 0 is simply all all rationals (in reduced form) whose numerator is congruent to $0 \bmod 4$.

Exercise 1.1.2. *Prove $|\cdot|_p$ is an absolute value on $\mathbb{Q}$.*

Recall, for a space R with an absolute value $|\cdot|$, one can define Cauchy sequences (x_n) in R—namely, for any $\epsilon > 0$, $|x_m - x_n| < \epsilon$ for all m, n large. One forms the completion of R with respect to $|\cdot|$ by taking equivalence classes of Cauchy sequences. Everyone knows that the completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$ is $\mathbb{R}$.

Definition 1.1.3. *The field $\mathbb{Q}_p$ of **p-adic numbers** is defined to be the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.*

The usual way to write down an explicit p-adic number is the following. Consider a sequence in $\mathbb{Q}$ given by

$$\begin{aligned}
x_0 &= a_{-d}p^{-d} + a_{1-d}p^{1-d} + \cdots + a_0 \\
x_1 &= a_{-d}p^{-d} + a_{1-d}p^{1-d} + \cdots + a_0 + a_1 p \\
x_2 &= a_{-d}p^{-d} + a_{1-d}p^{1-d} + \cdots + a_0 + a_1 p + a_2 p^2 \\
&\ \vdots
\end{aligned}$$

where $d \in \mathbb{Z}$ is fixed and each $0 \leq a_i < p$. Then $|x_{n+1} - x_n|_p = |a_{n+1}p^{n+1}|_p = \frac{1}{p^{n+1}}$ (unless $x_{n+1} = x_n$, in which case it is of course 0). Hence $x = (x_n)$ is a Cauchy sequence, and we can write it more succinctly as a formal Laurent series

$$x = a_{-d}p^{-d} + a_{1-d}p^{1-d} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots. \tag{1.1}$$

Assuming $a_{-d} \neq 0$, we see that $|x|_p = p^d$.

That any p-adic number can be written in the above form, follows from this simple exercise.

Exercise 1.1.4. *Suppose (x_n) is a Cauchy sequence in $(\mathbb{Q}, |\cdot|_p)$. Show that $|x_n - x|_p \to 0$ for some $x \in \mathbb{Q}_p$ of the form* (1.1).

Hence, the $\mathbb{Q}_p$'s are an arithmetic analogue of $\mathbb{R}$, just being completions of the absolute values on $\mathbb{Q}$ ($\mathbb{Q}$ is already complete with respect to the trivial absolute value—$\mathbb{Q}$ is totally disconnected with respect to $|\cdot|_0$). This approach to constructing $\mathbb{Q}_p$ gives both an absolute value and a topology on $\mathbb{Q}_p$, which are the most important things to understand about $\mathbb{Q}_p$.

Precisely, write any $x \in \mathbb{Q}_p$ as

$$x = a_m p^m + a_{m+1}p^{m+1} + \cdots,\ \ a_m \neq 0$$

for some $m \in \mathbb{Z}$. Then we define the **p-adic (exponential) valuation**(or **ordinal**) of x to be

$$\operatorname{ord}_p(x) = m.$$

Then

$$|x|_p = p^{-m} = p^{-\operatorname{ord}_p(x)}.$$

Definition 1.1.5. *The* **ring of integers** *of $\mathbb{Q}_p$, or the* **p-adic integers***, are*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \operatorname{ord}_p(x) \geq 0\} = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

Proposition 1.1.6. *$\mathbb{Z}_p$ is a closed (topologically) subring of $\mathbb{Q}_p$.*

Proof. That $\mathbb{Z}_p$ is closed is immediate from the definition since $x \mapsto |x|_p$ is continuous. Observing that

$$\mathbb{Z}_p = \left\{ \sum_{n \geq 0} a_n p^n \right\},$$

it is easy to see $\mathbb{Z}_p$ is a ring. □

Corollary 1.1.7. *The group of units $\mathbb{Z}_p^\times$ of $\mathbb{Z}_p$ is*

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : \operatorname{ord}_p(x) = 0\} = \{x \in \mathbb{Q}_p : |x|_p = 1\}.$$

Proof. Suppose $x \in \mathbb{Z}_p$ is invertible, i.e., $x^{-1} \in \mathbb{Z}_p$. Then

$$|x|_p |x^{-1}|_p = |1|_p = 1.$$

However $x, x^{-1} \in \mathbb{Z}_p$ implies $|x|_p$, $|x^{-1}|_p \leq 1$. Thus $|x|_p = |x^{-1}|_p = 1$. Hence $\mathbb{Z}_p^\times \subseteq \{x \in \mathbb{Q}_p : |x|_p = 1\}$.

Similarly, if $|x|_p = 1$, we see $|x^{-1}|_p = 1$ so $x \in \mathbb{Z}_p^\times$. □

Exercise 1.1.8. *Let $p = 5$. Determine $\operatorname{ord}_p(x)$ and $|x|_p$ for $x = 4, 5, 10, \frac{217}{150}, \frac{60}{79}$. Describe the (open) ball of radius $\frac{1}{10}$ centered around 0 in $\mathbb{Q}_p$.*

Exercise 1.1.9. *Let $x \in \mathbb{Q}$ be nonzero. Show*

$$|x|_\infty \cdot \prod_p |x|_p = 1.$$

This result will be important for us later.

Despite the fact that $\mathbb{R}$ and $\mathbb{Q}_p$ are analogous in the sense that they are both completions of nontrivial absolute values on $\mathbb{Q}$, there are a couple of fundamental ways in which the p-adic absolute value and induced topology are different from the usual absolute value and topology on $\mathbb{R}$.

Definition 1.1.10. *Let $|\cdot|$ be an absolute value on a field F. If $|x + y| \leq \max\{|x|, |y|\}$, we say $|\cdot|$ is* **nonarchimedean***. Otherwise $|\cdot|$ is* **archimedean***.*

The nonarchimedean triangle inequality, $|x + y| \leq \max\{|x|, |y|\}$, is called the **strong triangle inequality**.

Proposition 1.1.11. *$|\cdot|_\infty$ is archimedean but $|\cdot|_p$ is nonarchimedean for each p.*

Proof. Everyone knows $|\cdot|_\infty$ or $\mathbb{Q}$ or $\mathbb{R}$ is archimedean—this is what we are use to and the proof is just $|1+1|_\infty = 2 > 1 = \max\{|1|_\infty, |1|_\infty\}$.

Now let's show $|\cdot|_p$ is nonarchimedean on $\mathbb{Q}$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ ($\mathbb{Q}_p$ is the completion of $\mathbb{Q}$), this will imply $|\cdot|_p$ is nonarchimedean on $\mathbb{Q}_p$ also. Let $x, y \in \mathbb{Q}$. Write $x = p^m \frac{a}{b}$, $y = p^n \frac{c}{d}$, where a, b, c, d are relatively prime to p, and $m, n \in \mathbb{Z}$. Without loss of generality, assume $m \leq n$. Then we can write

$$x + y = p^m \left(\frac{a}{b} + p^{n-m} \frac{c}{d} \right) = p^m \frac{ad + p^{n-m} bc}{bd}.$$

Since $n \geq m$, the numerator on the right is an integer. The denominator are relatively prime to p since b, d are, though the numerator is possibly divisible by p (though only if $n = m$ and $p|(ad+bc)$). This means that we can write $x + y = p^{m+k} \frac{e}{f}$ where $e, f \in \mathbb{Z}$ are prime to p and $k \geq 0$. Thus

$$|x + y|_p = p^{-m-k} \leq p^{-m} = \max\left\{p^{-m}, p^{-n}\right\} = \max\{|x_p|, |y_p|\}$$

□

Notice that our proof shows that we actually have equality $|x+y|_p = \max\{|x|_p, |y|_p\}$ (since $k = 0$ above) except possibly in the case $|x|_p = |y|_p$.

Exercise 1.1.12. *Find two integers $x, y \in \mathbb{Z}$ such that*
(i) $|x|_3 = |y|_3 = \frac{1}{3}$ *but* $|x+y|_3 = \frac{1}{9}$.
(ii) $|x|_3 = |y|_3 = |x+y|_3 = \frac{1}{3}$.

Proposition 1.1.13. *Every ball $B_r(x)$ in $\mathbb{Q}_p$ is both open and closed. Thus the singleton sets in $\mathbb{Q}_p$ are closed.*

Using the fact that the balls are closed, one can show that $\mathbb{Q}_p$ is *totally disconnected*, i.e., its connected components are the singleton sets. However the singleton sets are not open, as that would imply $\mathbb{Q}_p$ has the discrete topology, i.e., every set would be both open and closed.

Proof. Each ball is open by definition. The following two exercises show $B_r(x)$ is also closed.

Then for any $x \in \mathbb{Q}_p$, the intersection of the closed sets $\bigcap_{r>0} B_r(x) = \{x\}$, which must be closed. □

Exercise 1.1.14. *Show* $B_r(x) = x + B_r(0) = \{x + y : y \in B_r(0)\}$.

Exercise 1.1.15. *Show that $B_r(0)$ is closed for any $r \in \mathbb{R}$.*

Your proof of the second exercise should make use of the fact that $|\cdot|_p$ is a *discrete* absolute value, i.e., the valuation $\mathrm{ord}_p : \mathbb{Q}_p \to \mathbb{R}$ actually has image $\mathbb{Z}$, which is a discrete subset of $\mathbb{R}$. In other words, the image of $|\cdot|_p = p^{-\mathrm{ord}_p(\cdot)}$, namely $p^{\mathbb{Z}}$, is discrete in $\mathbb{R}$ except for the limit point at 0. On the other hand, the image of the ordinary absolute value $|\cdot|_\infty$ on $\mathbb{R}$ is a *continuous* subset of $\mathbb{R}$, namely $\mathbb{R}_{\geq 0}$.

Another strange, but nice thing, about analysis on $\mathbb{Q}_p$ is that a series $\sum x_n$ converges if and only if $x_n \to 0$ in $\mathbb{Q}_p$.

While these are some very fundamental differences between $\mathbb{R}$ and $\mathbb{Q}_p$, you shouldn't feel that $\mathbb{Q}_p$ is too unnatural—just different from what you're familiar with. To see that $\mathbb{Q}_p$ isn't too strange, observe the following:

Proposition 1.1.16. *$\mathbb{Q}_p$ and $\mathbb{R}$ are both Hausdorff and locally compact, but not compact.*

Proof. The results for $\mathbb{R}$ should be familiar, so we will just show them for $\mathbb{Q}_p$.

Recall a space is Hausdorff if any two points can be separated by open sets. $\mathbb{Q}_p$ is Hausdorff since it is a metric space: namely if $x \neq y \in \mathbb{Q}_p$, let $d = d(x, y) = |x + y|_p$. Then for $r \leq \frac{d}{2}$, $B_r(x)$ and $B_r(y)$ are open neighborhoods of x and y which are disjoint.

Recall a Hausdorff space is locally compact if every point has a compact neighborhood. Around any $x \in \mathbb{Q}_p$, we can take the closed ball $\overline{B}_r(x)$ of radius r. This is a closed and (totally) bounded set in a complete metric space, and therefore compact. (In fact one could also take the open ball $\overline{B}_r(x)$, since we know it is closed from the previous exercise.)

Perhaps more instructively, one can show $\overline{B}_r(x)$ is sequentially compact in $\mathbb{Q}_p$, which is equivalent to compactness being a metric space. We may take a specific r if we want, say $r = 1$. Further since $\overline{B}_1(x) = x + \overline{B}_1(0)$ by the exercise above, it suffices to show $\overline{B}_1(0) = \{x \in \mathbb{Q}_p : |x|_p \leq 1\} = \mathbb{Z}_p$ is sequentially compact. If

$$
\begin{aligned}
x_1 &= a_{10} + a_{11}p + a_{12}p^2 + \cdots \\
x_2 &= a_{20} + a_{21}p + a_{22}p^2 + \cdots \\
x_3 &= a_{30} + a_{31}p + a_{32}p^2 + \cdots \\
&\vdots
\end{aligned}
$$

is a Cauchy sequence, then for any $\epsilon > 0$, there is an $N \in \mathbb{N}$ such that $|x_m - x_n|_p < \epsilon$ for all $m, n > N$. Take $\epsilon = p^{-r}$ for $r > 0$. Then $|x_m - x_n|_p < \epsilon = p^{-r}$ means $x_m \equiv x_n \bmod p^{r+1}$, i.e., the coefficients of $1, p, p^2, \ldots, p^r$ must be the same for all x_m, x_n with $m, n > N$. Let $a_0, a_1, \ldots, a_r$ denote these coefficients. We can do this for larger and larger r (note that $a_0, \ldots, a_{r-1}$ will never change) to get a sequence (a_n), and then it is clear that the above sequence converges to

$$x = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p.$$

This provides a second proof of local compactness.

To see $\mathbb{Q}_p$ is not compact, observe the sequence $x_1 = p^{-1}$, $x_2 = p^{-2}$, $x_3 = p^{-3}, \ldots$ has no convergent subsequence. Geometrically, $|x_n| = p^n$, so this is a sequence of points getting further and further from 0, and the distance to 0 goes to infinity. □

We remark that $\mathbb{Q}$, with either usual subspace topology coming from $\mathbb{R}$ or the one coming from $\mathbb{Q}_p$, is a space which is not locally compact. The reason is any open neighborhood about a point is not complete—the limit points are contained in the completion of $\mathbb{Q}$ (w.r.t. to whichever absolute value we are considering), but not in $\mathbb{Q}$. (The trivial absolute value $|\cdot|_0$ induces the discrete topology on $\mathbb{Q}$, meaning single points are open sets, so it is trivially locally compact.)

The general definition of a **local field** is a locally compact field with a non-discrete topology, hence we see that $\mathbb{Q}_p$ and $\mathbb{R}$ are local fields, whereas $\mathbb{Q}$ (with the usual topology) is not. Any local field of characteristic 0 will be a finite extension of $\mathbb{Q}_p$ or $\mathbb{R}$. These will be the completions of number fields (a finite extension of $\mathbb{Q}$), which are in contrast called **global fields**.

To try to minimize the background required, we will mostly work with $\mathbb{Q}_p$, though the theory we develop extends without difficulty to any finite extension.

1.2 Representation theory

Definition 1.2.1. *Let G be a group and V be a vector space over a field F. A* **representation** π *of G on V is a homomorphism*

$$\pi : G \to \mathrm{GL}(V),$$

where $\mathrm{GL}(V)$ denotes the group of automorphisms of V. The representation is denoted by (π, V), π, or sometimes just V. Here V is called the **representation space** *of V.*

*If $\dim V = n < \infty$, we say π is an n-***dimensional representation** *over F. Otherwise, we say π is* **infinite dimensional**. *If π is a 1-dimesional representation, we also refer to π as a* **(linear) character**.

Example 1.2.2. *Let G and V be arbitrary. The map $\pi : G \to \mathrm{GL}(V)$ given by $\pi(g) = \mathrm{id}$ is always a representation, called the* **trivial representation** *of G on V.*

If we simply say the trivial representation *of G, without other context, it is taken for granted we mean the 1-dimensional trivial representation $\pi : G \to \mathrm{GL}_1(F)$.*

Example 1.2.3. *Let $G = C_n$, the cyclic group of order n, and take $F = \mathbb{C}$. Write $G = \langle x | x^n = 1\rangle$. Then the map*

$$\pi_1 : G \to \mathrm{GL}(\mathbb{C}) = \mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^\times \quad \textit{given by} \quad \pi_1(x^j) = e^{2\pi i j/n}$$

is a representation (in fact, linear character) of G. Note that since π_1 is a homomorphism, it is determined by its values on a set of generators, so one can define π_1 simply by $\pi_1(x) = e^{2\pi i/n}$.

The homomorphism

$$\pi_2 : G \to \mathrm{GL}(\mathbb{C}^2) = \mathrm{GL}_2(\mathbb{C}) \quad \textit{defined by} \quad \pi_2(x) = \begin{pmatrix} e^{2\pi i k_1/n} & \\ & e^{2\pi k_2/n} \end{pmatrix}$$

is a 2-dimensional representation of G for any fixed $k_1, k_2 \in \mathbb{Z}$. One can analogously define an n-dimensional representation of C_n.

While π_2 in the example above gives an action of C_n on a 2-dimensional space $V = \mathbb{C}^2$, the action is entirely determined by what it does to the two orthogonal subspaces $\mathbb{C}e_1$ and $\mathbb{C}e_2$, where $\{e_1, e_2\}$ is the standard basis for V. Thus we should be able to decompose π_2 into two 1-dimensional representations.

Definition 1.2.4. *Let (π, V) be a representation of a group G. We say W is a* **(G-)invariant subspace** *of V if $\{\pi(g)w : g \in G, w \in W\} \subseteq W$. A* **subrepresentation** *of a representation (π, V) of a group G is an invariant subspace W of V together with the homomorphism*

$$\pi_W : G \to \mathrm{GL}(W) \quad \textit{given by} \quad \pi_W(g)w = \pi(g)w.$$

For a subrepresentation W, the **quotient** *of (π, V) by (π_W, W) is the representation*

$$\pi^W : G \to \mathrm{GL}(V/W) \quad \textit{given by} \quad \pi^W(g)(v + W) = \pi(g)v + W.$$

If $V = W_1 \oplus \cdots \oplus W_k$ with each W_i invariant, we say π is a **direct sum** *of $\pi_{W_1}, \ldots \pi_{W_k}$ and write*

$$\pi = \pi_{W_1} \oplus \cdots \oplus \pi_{W_k}.$$

Since the maps π_W and π^W are naturally defined given W, we typically just refer to the subrepresentation and quotient representation as W and V/W.

Exercise 1.2.5. *(i) Check the quotient is a well-defined representation.*

(ii) For π_2 from the previous example, determine the subrepresentations and their quotients. Is π_2 a direct sum?

For any representation (π, V), the subspaces $\{0\}$ and V are always invariant.

Definition 1.2.6. *We say (π, V) is* **irreducible** *if there are no invariant subspaces other than $\{0\}$ and V.*

Example 1.2.7. *Any 1-dimensional representation is irreducible. In particular, the trivial one is.*

Proposition 1.2.8. *Let G be a finite group and (π, V) be a representation of G. If π is irreducible, then π is finite dimensional.*

This is of course not true for general groups, though if G is *compact*, e.g., Gal $= \mathrm{SO}(2)$, then the irreducible *continuous* representations are finite dimesional.

Proof. Let $v_0 \in V$ be nonzero. Then the linear span W of $\langle \pi(g)v_0 : g \in G\rangle$ is a invariant subspace. To see this take any $w \in W$. Then we can write $w = \sum c_i \pi(g_i)v_0$, where this sum is finite. For any $g \in G$, we see

$$\pi(g)w = \sum c_i \pi(gg_i)v_0 \in W.$$

Since $\pi(1)v_0 = v_0$, we see $W \neq \{0\}$. Hence by irreducibility, $W = V$, but it is clear W is finite dimensional. $\square$

The basic problem in representation theory is to classify all irreducible representations of G. In working with groups with more structure, such as topological groups or algebraic (matrix) groups, one typically restricts this question to a certain class of representations, such as *continuous* or *smooth* representations, that are more natural for the groups at hand. We will wait to discuss this until the next chapter.

All representations of finite groups over $\mathbb{C}$ decompose into a direct sum of irreducible representations, so in this case, knowing the irreducible representations of a group tells us all representations of a group. While this is not true in general, this classification is still crucial to understanding the representation theory of the group.

There are meaningless ways to get new representations out of old ones, such as replacing F or V by something which is isomorphic. A slightly less trivial, but still essentially meaningless, way to get a new representation out of an old one is by conjugation. For example, if π_2 is as in the previous example, we can replace π_2 by $\pi_2^\gamma(g) = \gamma^{-1}\pi_2(g)\gamma$ for any $\gamma \in \mathrm{GL}_2(\mathbb{C})$. If $\gamma = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$, then π_2^γ simply interchanges k_1 and k_2. More generally, conjugation can be viewed as a special case of composing the representation with either an automorphism of V or an automorphism of G.

Thus this classification of irreducible representations should only be up to a certain notion of equivalence.

Definition 1.2.9. *Let* (π_1, V_1) *and* (π_2, V_2) *be representations of* G*. A linear transformation* $A : V_1 \to V_2$ *is an* **intertwining map** *if*

$$\pi_2(g)A = A\pi_1(g), \quad g \in G.$$

The set of all such intertwining maps is denoted $\mathrm{Hom}_G(\pi_1, \pi_2) = \mathrm{Hom}_G(V_1, V_2)$*. We also write* $\mathrm{End}_G(\pi) = \mathrm{Hom}_G(\pi, \pi)$ *and* $\mathrm{End}_G(V) = \mathrm{Hom}_G(V, V)$*. We omit the subscripts* G *when understood.*

We say π_1 *and* π_2 *are* **equivalent** *if* $\mathrm{Hom}_G(\pi_1, \pi_2)$ *contains an invertible transformation* $A : V_1 \to V_2$*. In this case we write* $\pi_1 \cong \pi_2$*.*

Note we always have $0 \in \mathrm{Hom}(\pi_1, \pi_2)$.

Example 1.2.10. *Let* $G = C_n = \langle x \rangle$,

$$\pi_1 : G \to \mathrm{GL}_1(\mathbb{C}) \quad \textit{given by} \quad \pi_1(x) = e^{2\pi i/n}$$

$$\pi_2 : G \to \mathrm{GL}_1(\mathbb{C}) \quad \textit{given by} \quad \pi_2(x) = e^{-2\pi i/n}$$

$$\pi_3 : G \to \mathrm{GL}_2(\mathbb{C}) \quad \textit{given by} \quad \pi_3(x) = \begin{pmatrix} e^{2\pi i/n} & \\ & e^{-2\pi i/n} \end{pmatrix}$$

$$\pi_4 : G \to \mathrm{GL}_2(\mathbb{C}) \quad \textit{given by} \quad \pi_4(x) = \begin{pmatrix} e^{-2\pi i/n} & \\ & e^{2\pi i/n} \end{pmatrix}.$$

Let us assume $n > 2$ *so* $e^{2\pi i/n} \neq e^{-2\pi i/n}$.

Then

$$\mathrm{End}(\pi_1) = \mathrm{Hom}(\pi_1, \pi_1) = \{A \in M_{1\times 1}(\mathbb{C}) : \pi_1(g)A = A\pi_1(g)\} = \mathbb{C}$$

Note if $A \in \mathrm{Hom}(\pi_1, \pi_2)$ *this means* $A \in \mathbb{C}$ *such that*

$$\pi_2(x)A = A\pi_1(x) \textit{ for } v \in \mathbb{C} \implies e^{-2\pi i/n}A = Ae^{2\pi i/n} \implies A = 0,$$

i.e., $\mathrm{Hom}(\pi_1, \pi_2) = \{0\}$.

Now let's determine $\mathrm{Hom}(\pi_1, \pi_3)$*. Suppose* $A = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} : \mathbb{C} \to \mathbb{C}^2$*. Then* $A \in \mathrm{Hom}(\pi_1, \pi_3)$ *means, for all* $j \in \mathbb{Z}$,

$$\pi_3(x^j)A = A\pi_1(x^j) \iff \begin{pmatrix} e^{2\pi ij/n} & \\ & e^{-2\pi ij/n} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} e^{2\pi ij/n} \iff a_2 = 0.$$

Hence we see that $\mathrm{Hom}(\pi_1, \pi_3) = \left\{ \begin{pmatrix} a \\ 0 \end{pmatrix} : a \in \mathbb{C} \right\} \simeq \mathbb{C}$.

Finally, we determine $\mathrm{Hom}(\pi_3, \pi_4)$*. Suppose* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \mathbb{C}^2 \to \mathbb{C}^2$*. Then* $A \in \mathrm{Hom}(\pi_3, \pi_4)$ *means, for all* $j \in \mathbb{Z}$,

$$\pi_4(x^j)A = A\pi_3(x^j) \iff \begin{pmatrix} e^{-2\pi ij/n} & \\ & e^{2\pi ij/n} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e^{2\pi ij/n} & \\ & e^{-2\pi ij/n} \end{pmatrix}.$$

It is easy to see this means

$$\mathrm{Hom}(\pi_3, \pi_4) = \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} : b, c \in \mathbb{C} \right\} \simeq \mathbb{C} \oplus \mathbb{C}.$$

Since this contains invertible elements in $M_2(\mathbb{C})$*, we see* π_3 *and* π_4 *are equivalent.*

Exercise 1.2.11. *Keep the notation of the previous example.*

(i) Determine $\mathrm{End}(\pi_3)$ *and* $\mathrm{Hom}(\pi_3, \pi_2)$*.*

(ii) Consider the representation

$$\pi_5 : G \to \mathrm{GL}_2(\mathbb{C}) \quad \text{given by} \quad \pi_4(x) = \begin{pmatrix} e^{2\pi i/n} & \\ & e^{2\pi i/n} \end{pmatrix}.$$

Determine $\mathrm{End}(\pi_5)$ *and* $\mathrm{Hom}(\pi_5, \pi_3)$*.*

As you might guess from the above example, the space $\mathrm{Hom}(\pi_1, \pi_2)$ tell us when π_1 is (up to equivalence) a subrepresentation of π_2, or more generally, how many subrepresentations π_1 and π_2 have in common. For now, let us just state what happens for finite groups.

Proposition 1.2.12. *Let G be a finite group and (π_1, V_1), (π_2, V_2) be finite-dimensional representations over $\mathbb{C}$.*

(i) **(Schur's lemma)** *Suppose π_1 and π_2 are irreducible. Then* $\mathrm{Hom}(\pi_1, \pi_2) = \{0\}$ *unless $\pi_1 \cong \pi_2$, in which case* $\mathrm{Hom}(\pi_2, \pi_2) \simeq \mathbb{C}$*.*

(ii) Suppose π_1 is irreducible. Then $\mathrm{Hom}(\pi_1, \pi_2) \simeq \mathbb{C}^n$ *where n is the number of times π_1 appears (up to equivalence) in the direct sum decomposition (which is unique up to equivalence) of π_2.*

(iii) Suppose $\pi_1 \cong \rho_1 \oplus \cdots \oplus \rho_l$ and $\pi_2 \cong \tau_1 \oplus \cdots \oplus \tau_k$ with each ρ_i, τ_j irreducible. Then $\mathrm{Hom}(\pi_1, \pi_2) \simeq \mathbb{C}^n$ *where n is the number of pairs (i, j) such that $\rho_i \cong \tau_j$.*

(iv) π_1 is irreducible if and only if $\mathrm{Hom}(\pi_1, \pi_1) \simeq \mathbb{C}$*.*

We will show Schur's lemma, in greater generality, later in this course. Parts (ii) and (iii) are simple generalizations of (i), and (iv) a consequence of (iii).

Before we move on to the next topic, here are a couple other examples of finite-dimensional representations.

Example 1.2.13. *Let $G = \mathrm{GL}_n(F)$ or $\mathrm{SL}_n(F)$, where F is a field. The map $\pi : G \to \mathrm{GL}_n(F)$ given by $\pi(g) = g$ is an irreducible n-dimensional representation of G, called the* **standard representation** *of G.*

The map $\check{\pi} : G \to \mathrm{GL}_n(F)$ given by $\pi(g) = {}^t g^{-1}$ is also an n-dimensional representation of G, called the **contragredient representation** *associated to π. (One can make this definition for any G, π).*

A nontrivial 1-dimensional representation of G is given by the map $g \mapsto \det(g)$.

Example 1.2.14. *Let π be the standard representation of $G = \mathrm{GL}_2(F)$, and let e_1, e_2 be the standard basis for $V = F^2$. Let $\mathrm{Sym}^2(V)$ be the 3-dimensional vector space generated by the symmetric algebra $e_1 \otimes e_1$, $e_1 \otimes e_2 = e_2 \otimes e_1$, $e_2 \otimes e_2$. The symmetric square representation $\mathrm{Sym}^2(\pi) : G \to \mathrm{GL}_3(F) = \mathrm{GL}(\mathrm{Sym}^2(v))$ is given by*

$$\mathrm{Sym}^2(\pi)(g)(e_i \otimes e_j) = g \cdot e_i \otimes g \cdot e_j.$$

More explicitly, using the above ordered basis for $\mathrm{Sym}^2(V)$, we have

$$\mathrm{Sym}^2(\pi) \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 & ab & b^2 \\ 2ac & ad + bc & 2bd \\ c^2 & cd & d^2 \end{pmatrix}.$$

This is irreducible (except in the degenerate case when $F = \mathbb{F}_2$ and $G \simeq S_3$).

1.2.1 Induction and restriction

Let H be a subgroup of G such that $H \neq G$. For simplicity, we assume G is finite in this section.

Induction and restriction allow us to transfer representations from H to G and vice versa. Restriction is trivial.

Definition 1.2.15. *Let π be a representation of G. The* **restriction** *π_H of π to H is simply the representation defined by*

$$\pi_H(h) = \pi(h).$$

Example 1.2.16. *Let $\pi : G \to \mathrm{GL}_n(F)$. Since $\pi(1) = I_n$, the restriction $\pi_{\{1\}}$ of π to the trivial subgroup decomposes as a direct sum n-copies of the trivial representation. (The only irreducible representation of $\{1\}$ is the trivial one.)*

Conversely, given a representation (ρ, W) of H, one might ask to construct a representation π of G such that $\pi_H = \rho$. This would mean that one could extend the homomorphism $\rho : H \to \mathrm{GL}(W)$ to a homomorphism $\pi : G \to \mathrm{GL}(W)$, which is not always possible. However, what we can always do is extend ρ to a homomorphism $\pi : G \to \mathrm{GL}(V)$ where V is some superspace of W. In particular, one can formally take $V = \bigoplus_{g \in G/H} gW$, where $gW = \{gw : w \in W\} \simeq W$. Then one defines the action $\pi(g)$ on V by

$$\pi(g)g'w = g''\rho(h)w \in g''W, \quad \text{where} gg' = g''h.$$

Exercise 1.2.17. *Check that π is a well defined representation of G, called the representation induced from ρ.*

In particular, if we restrict π to H and $g' = 1$, then we see

$$\pi(h)w = \rho(h)w$$

so the restriction π_H contains ρ as a subrepresentation. However, by definition π_H acts on a larger space V, so $\pi_H \neq \rho$, i.e., the quotient of π_H by ρ is nontrivial. In this sense, we see induction is a converse construction to restriction.

There is another way to define induction, which is more suitable for our point of view.

Definition 1.2.18. *Let (ρ, W) be a representation of H. The* **induction** *of ρ from H to G is the representation $(\mathrm{Ind}_H^G(\rho), V)$ where*

$$V = \{f : G \to W | f(hg) = \rho(h)f(g)\}$$

and

$$\mathrm{Ind}_H^G(\rho)(g)f(x) = f(xg).$$

In general, one might want to restrict to functions $f : G \to W$ of a certain type (e.g., continuous or smooth), but these restrictions are vacuous for finite groups.

Example 1.2.19. *Consider C_3 as a subgroup of the symmetric (or dihedral if you prefer) group S_3 of order 6. Write $S_3 = \langle \sigma, \tau | \sigma^2 = \tau^3 = 1, \sigma\tau\sigma = \tau^{-1}\rangle$ so $C_3 = \langle \tau \rangle$. Let (ρ, W) be the 1-dimensional representation of C_3 over $\mathbb{C}$ given by $W = \mathbb{C}$ and*

$$\rho(\tau^j) = \zeta^j, \quad \zeta = e^{2\pi i/3}.$$

Set
$$V = \{f : S_3 \to W | f(hg) = \rho(h)f(g)\}.$$
There are two cosets in $C_3\backslash S_3$*, represented by* 1 *and* σ*. Hence* $f \in V$ *means*
$$f(\tau^j) = \rho(\tau^j)f(1) = \zeta^j f(1)$$
and
$$f(\tau^j\sigma) = \zeta^j f(\sigma).$$
Conversely, these conditions imply $f \in V$*, whence* $f \in V$ *is determined by* $f(1)$ *and* $f(\tau)$*. In particular,* $\dim V = 2$.

We can use this to write $\pi = \mathrm{Ind}_{C_3}^{S_3}(\rho)$ *in matrix form. Namely, let* $f_1, f_2 \in V$ *be defined by* $f_1(1) = f_2(\sigma) = 1$*,* $f_1(\sigma) = f_2(1) = 0$*. Then*
$$\pi(\sigma)f_1(1) = f_1(\sigma) = 0, \quad \pi(\sigma)f_1(\sigma) = f_1(\sigma^2) = f_1(1) = 1,$$
which implies
$$\pi(\sigma)f_1 = 0 \cdot f_1 + 1 \cdot f_2.$$
A similar computation shows
$$\pi(\sigma)f_2 = 1 \cdot f_1 + 0 \cdot f_2.$$
Consequently, with respect to the ordered basis f_1, f_2*,*
$$\pi(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$
Next note
$$\pi(\tau)f_1(1) = f_1(\tau) = \zeta, \quad \pi(\tau)f_1(\sigma) = f_1(\sigma\tau) = f_1(\tau^2\sigma) = 0,$$
so
$$\pi(\tau)f_1 = \zeta \cdot f_1 + 0 \cdot f_2.$$
Similarly we see
$$\pi(\tau)f_2 = 0 \cdot f_1 + \zeta^2 \cdot f_2.$$
Thus we can write
$$\pi(\tau) = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{pmatrix}.$$
Since σ, τ *generate* S_3*, this determines* π *on any element of* S_3*. Observing* π *is* faithful*, i.e., injective, we see* π *gives a* matrix realization *for* S_3 *in* $\mathrm{GL}_2(\mathbb{C})$.

Exercise 1.2.20. *With* π *the induced representation of* S_3 *in the previous example, compute* $\mathrm{Hom}(\pi, \pi)$ *and conclude* π *is irreducible.*

Exercise 1.2.21. *Show* $\dim \mathrm{Ind}_H^G(\rho) = |G/H| \cdot \dim \rho$.

Exercise 1.2.22. *Compute* $\mathrm{Ind}_{C_3}^{S_3}(1)$ *where* 1 *denotes the (1-dimensional) trivial representation of* C_3.

Exercise 1.2.23. *Let* ρ *be a non-trivial representation of the Klein group* V_4*. Compute* $\mathrm{Ind}_{V_4}^{A_4}(\rho)$.

1.2.2 Character theory

One of the main tools to study representations, particularly of finite groups, is to look at their characters. Again, we will restrict to the case of finite groups in this section, and all our representations will be finite dimensional.

Definition 1.2.24. *Let (π, V) be a representation of G over F. The* character χ_π *of π is the function $\chi_\pi : G \to F$ defined by*

$$\chi_\pi(g) = \mathrm{tr}\pi(g) = \sum_{e_i} (\pi(g)e_i, e_i),$$

where $(\ ,\ )$ is an inner product on V and e_i an orthonormal basis.

We remark that χ_π does not depend upon on the choice of inner product or basis. In fact, it only depends upon the equivalence class of π, making it a useful invariant.

Since the trace is conjugacy invariant, any character χ_π of G is a *class function* on G, i.e., $\chi_\pi(g)$ only depends upon the conjugacy class of g in G.

Example 1.2.25. *If $G = \mathrm{GL}_n(F)$ or $\mathrm{SL}_n(F)$ and π is the standard representation on F^n, then $\chi_\pi(g) = \mathrm{tr}(g)$.*

Example 1.2.26. *If π is a 1-dimensional representation of G, then $\chi_\pi(g) = \pi(g)$. This explains why a* 1*-dimensional representation is also called a character.*

Example 1.2.27. *Suppose π is a n-dimensional representation. Then $\pi(1)$ is the identity of $\mathrm{GL}_n(F)$, so $\chi_\pi(1) = n = \dim \pi$. We also call $\chi_\pi(1)$ the* **degree** $\deg \chi_\pi$ *of χ_π.*

For the rest of the section, **we assume** $F = \mathbb{C}$.

Theorem 1.2.28. *Let $\chi_1, \ldots, \chi_r$ be the irreducible characters of G, i.e., the (finite number of) characters of irreducible representations of G. Then*

(i) (First orthogonality relation) For any i, j,

$$\sum_{g \in G} \chi_i(g)\chi_j(g^{-1}) = \delta_{ij}|G|.$$

(ii) (Second orthogonality relation) For any $g, h \in G$,

$$\sum_{i=1}^{r} \chi_i(g)\chi_i(h^{-1}) = \begin{cases} |C_G(g)| & \text{if } g \text{ is conjugate to } h \\ 0 & \text{else.} \end{cases}$$

(iii) $\chi_1, \ldots, \chi_r$ for a basis for the space of class functions on G. In particular, r is the number of conjugacy classes of G.

(iv)

$$\sum_{i=1}^{r} (\deg \chi_i)^2 = |G|.$$

These results can be found in any standard text on representation theory for finite groups.

All of these results are very useful, but (iii) and (iv) are particularly useful for determining the irreducible representations of G.

Example 1.2.29. *Suppose G is abelian of order n. Then each element of G is its own conjugacy classes, thus there are n irreducible representations by (iii). By (iv), the sum of their dimensions squared must be n, hence they are all 1-dimensional.*

In particular, for $G = C_n = \langle x \rangle$, consider the 1-dimensional representation given by $\pi_1(x) = \zeta = e^{2\pi i/n}$. Then the representations $\pi_j = \pi_i^j$ for $j = 0, 1, \ldots, n-1$ are all inequivalent, and hence are all irreducible representations of G.

Exercise 1.2.30. *Let G be any finite abelian group. Construct all irreducible representations of G.*

Example 1.2.31. *Let's determine all irreducible representations of S_3 over $\mathbb{C}$, and then compute their characters. Let π be as in Example 1.2.19.*

We already know 2 irreducible representations of S_3, namely the trivial one χ_0 and the 2-dimensional induced representation π from Example 1.2.19. By Theorem 1.2.28(iii), there is only 1 more irreducible representation of S_3, and by part (iv) of the same theorem, it must be 1-dimensional. Let us call it ψ.

Since a 1-dimensional representation of S_3 must have abelian image (it lies in $\mathrm{GL}_1(\mathbb{C})$), it must have nontrivial kernel. This kernel is a normal subgroup of S_3, of which the nontrivial ones are C_3 and S_3. If the kernel is S_3, then the representation must be trivial, so ψ must have kernel C_3, i.e., it descends to a representation of the quotient $S_3/C_3 \simeq C_2$. The only irreducible (which in this case is equivalent to 1-dimensional) representations of C_2 are the trivial one and the embedding of C_2 as $\{\pm 1\}$ in $\mathbb{C}^\times \simeq \mathrm{GL}_1(\mathbb{C})$.

Explicitly, we may write ψ as

$$\psi(\tau^j) = 1, \quad \psi(\sigma\tau^j) = -1$$

for any $j = 0, 1, 2$.

Thus χ_0, ψ, π are all irreducible representations of S_3. To compute the character of π, it suffices to determine its value on each of the conjugacy classes of S_3, of which there are 3. We may take for conjugacy class representatives $1, \sigma, \tau$.

It is often convenient to present the irreducible characters of S_3 as a **character table**, *which is a table with the rows indexed by the characters and the columns indexed by the conjugacy classes. For S_3, we see it looks like*

	1	σ	τ
χ_0	1	1	1
ψ	1	-1	1
χ_π	2	0	-1

Exercise 1.2.32. *Determine all irreducible representations of A_4 and compute the character table.*