Physics 509 Homework 6

Professor M. Stone
University of Illinois

Spring 2022

1 Group Theory in Theory

Before proving the following statements, we first prove one trivial lemma which will lessen our work.

Subgroup Lemma. H is a subgroup of G if and only if for all $h_1, h_2 \in H$, $h_1 h_2^{-1} \in H$.

Proof. If H is a group, then clearly $h_1 h_2^{-1} \in H$ by the closure property. Suppose $h_1, h_2 \in H$, then setting $h_1 = h_2 \implies h_1 h_1^{-1} = e \in H$; setting $h_1 = e$, $h_2 = h_1 \implies e h_1^{-1} = h_1^{-1} \in H$; and associativity follows since H is a subset of G (with the same binary operation). ■

(a) Note that if $h \in Z(G)$, then $hg = gh \implies h^{-1}hgh^{-1} = h^{-1}ghh^{-1} \implies gh^{-1} = h^{-1}g$, so $h^{-1} \in Z(G)$. Therefore, for any $h_1, h_2 \in H$, $(h_1 h_2^{-1})g = g(h_1 h_2^{-1})$ for any $g \in G$. H then is a subgroup of G by the subgroup lemma.

(b) If $h \in C_G(g)$, then $hg = gh \implies gh^{-1} = h^{-1}g$. Hence the subgroup lemma again shows H is a subgroup of G.

(c) Similarly, if $g \in C_G(H)$, then $gh = hg \implies hg^{-1} = g^{-1}h$ for any $h \in H$, so that if g_1, $g_2 \in C_G(H)$, then $g_1 g_2^{-1} h = g_1 g_2^{-1} h$ for all $h \in H$, which implies $C_G(H)$ is a subgroup of G.

(d) Clearly, if $g \in N_G(H)$ then $g^{-1} \in N_G(H)$. A straightforward application of the subgroup lemma again shows $N_G(H)$ is a subgroup of G. Furthermore, H is a normal subgroup of $N_G(H)$ since $h^{-1}Hh = H$ is trivially satisfied.

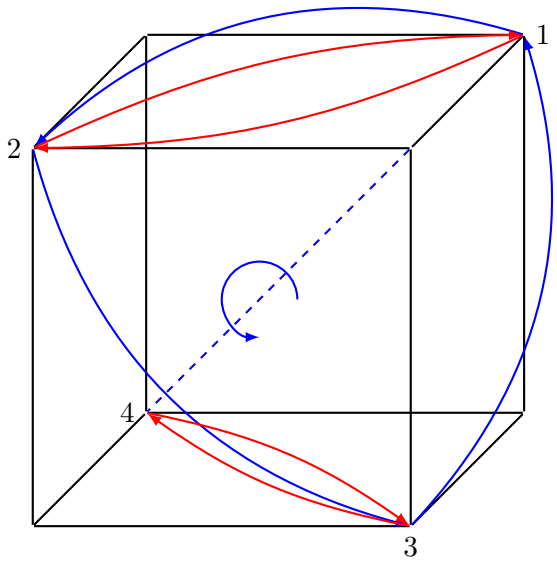
2 Group Theory in Practice

(a) The *dihedral group* D_n is generated by two elements, a and b, satisfying the relations $a^n = e$, $b^2 = e$, and $(ab)^2 = e$.

(i) To show that $|D_n| = 2n$, let $0 \leq m < n$. Then a^m accounts for n distinct elements. We further claim that $ba^m = a^{-m}b$,[1] so that any product of $a^m b$ can be expressed as a product with the b to the left. First, note the base case follows from $(ab)^2 = e \implies ab = b^{-1}a^{-1} = ba^{-1}$, since $b^{-1} = b$. Continuing inductively, we have

$$\begin{aligned} a^k b &= a a^{k-1} b \\ &= aba^{-(k-1)} \qquad \text{(inductive hypothesis)} \end{aligned}$$

[1] We use the obvious notation $a^{-m} \equiv (a^m)^{-1}$.



- b corresponds to a rotation by π around the vertical axis (not shown). It swaps two pairs of vertices in the top and bottom face of on the cube. In cycle notation, $b = (1\ 2)\,(3\ 4)$.
- c corresponds to a $2\pi/3$ rotation around the perpendicular to the plane containing vertices 1, 2, and 3 (perpendicular shown in dashed blue). $c = (1\ 2\ 3)$.

Figure 1: Isometries of the tetrahedron (inscribed in a cube) which depict the group elements of T_4.

$$= ba^{-1}a^{-(k-1)} \qquad \text{(base case)}$$
$$= ba^{-k}.$$

Since this accounts for an additional n elements, we have $|D_n| = 2n$.

(ii) The multiplication table for D_n is shown below (multiplication is by row then column).

	e	a	a^2	b	ba	ba^2
e	e	a	a^2	b	ba	ba^2
a	a	a^2	e	ba^2	b	ba
a^2	a^2	e	a	ba	ba^2	b
b	b	ba	ba^2	e	a	a^2
ba	ba	ba^2	b	a^2	e	a
ba^2	ba^2	b	ba	a	a^2	e

(b) We label the given permutations

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 4 & 8 & 5 & 7 & 2 & 3 \end{pmatrix} \qquad \text{and} \qquad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 4 & 1 & 8 & 9 & 6 & 7 & 2 \end{pmatrix}.$$

(i) Expressed in cycle notation these are

$$\pi_1 = (1\ 6\ 7\ 2)\,(3\ 4\ 8)\,(5) \qquad \text{and} \qquad \pi_2 = (1\ 3\ 4)\,(2\ 5\ 8\ 7\ 6\ 9)\,.$$

(ii) Writing all the cycles out as transpositions, we find

$$\pi_1 = (1\ 6)\,(6\ 7)\,(7\ 2)\,(3\ 4)\,(4\ 8) \implies \pi_1 \text{ is odd}$$
$$\pi_2 = (1\ 3)\,(3\ 4)\,(2\ 5)\,(5\ 8)\,(8\ 7)\,(7\ 6)\,(6\ 9) \implies \pi_2 \text{ is odd,}$$

where the parity of a permutation is defined by the parity of the number of transpositions.

(iii) Note that for a k-cycle σ_k, $\text{ord}(\sigma_k) = k$. For a permutation expressed as a product of cycles, $\pi = \sigma_{k_1}\sigma_{k_2}\cdots\sigma_{k_n}$, this generalizes to $\text{lcm}(k_1, k_2, \ldots, k_n)$. Therefore $\text{ord}(\pi_1) = \text{lcm}(\{4, 3, 1\}) = 12$ and $\text{ord}(\pi_2) = \text{lcm}(\{3, 6\}) = 6$.

(iv) Using the result in the previous part, one finds $\text{ord}\left((a_1\ a_2\ \cdots\ a_{2r})\,(b_1\ b_2\ \cdots\ b_r)\right) = 2r$.

(c) We next show that the *tetrahedral group* T is generated by two element, $\{b, c\} = b^2 = c^3 = (bc)^3 = e$. This can be done by either writing all of the combinations of group elements or drawing the rigid rotations of the tetrahedron (shown in figure 1). In cycle notation, the group elements are

$$\begin{aligned}
e &= (\ ) & cb &= (4\ 1)\,(1\ 3)\\
c &= (1\ 2)\,(2\ 3) & c^2b &= (4\ 2)\,(2\ 3)\\
c^2 &= (1\ 3)\,(3\ 2) & cbc &= (4\ 2)\,(2\ 1)\\
b &= (1\ 2)\,(3\ 4) & c^2bc &= (3\ 1)\,(2\ 4)\\
bc &= (3\ 2)\,(2\ 4) & cbc^2 &= (4\ 1)\,(3\ 2)\\
bc^2 &= (3\ 1)\,(1\ 4) & c^2bc^2 &= (2\ 1)\,(1\ 4)\,.
\end{aligned}$$

That these are the only elements of the group can be found by showing that the remaining formal combinations of a's and b's are all equivalent to a group element written above. To this end, one can easily check we have the following relations:

$$\begin{aligned}
cbcb &= bc^2 & bcb &= c^2bc^2\\
bc^2bc &= cbc^2 & bc^2bc^2 &= cb\\
bcbc^2 &= c^2bc & c^2bc^2b &= bc,
\end{aligned}$$

which confirms that T is indeed generated by the elements a and b. In group theory parlance, we say we have the following *presentation* of the group T_4,

$$\langle a, b \,|\, b^2 = c^3 = (bc)^3 = e\rangle.$$

3 An Application of Group Theory to Cryptography

(a) For any finite group G, it must be that $a^n = e$ for some integer n (pigeonhole principle). The smallest such n is known as the *order* of a in G, and is denoted $n \equiv \text{ord}(a)$. Then for any a^k with $0 \leq k < n$, $a^{-k} \equiv \left(a^k\right)^{-1} = a^{n-k}$, which likewise is a power of a; therefore, by the subgroup lemma, $\langle a \rangle \equiv \{a^k \mid k \in \mathbb{N}\}$, is a subgroup of G.

(b) We first show that $(\mathbb{Z}_p)^\times$ is a group. Clearly the set contains $(p-1)$ elements with associativity following immediately from the associativity of multiplication. Now any elements $a, b \in \{1, 2, \ldots, p-1\}$ will have a unique prime factorization, say $a = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$ and $b = s_1^{\beta_1} s_2^{\beta_2} \ldots s_\ell^{\beta_\ell}$, where q_i and s_i are primes less than p. Therefore, p does not divide the product ab, so that $ab \neq 0 \mod p$. This shows the set $\{1, 2, \ldots, p-1\}$ is closed under multiplication (modulo p). Furthermore, a corollary of Euclid's algorithm known as Bézout's identity[2] states that for any integers a and b, one can find integers x and y such that

$$ax + by = \gcd(a, b). \tag{1}$$

Therefore, there exists an x such that $ax = \gcd(a, p) = 1 \mod p$ (we can ensure $x \in \{1, 2, \ldots, p-1\}$ here simply by adding a multiple of p to it), which shows every element has an inverse and $(\mathbb{Z}_p)^\times$ is a group. We next prove *Fermat's little theorem*, which states that for any integer a and prime p, we have

$$a^{p-1} = 1 \mod p. \tag{2}$$

Proof using Lagrange's theorem. Consider the subgroup generated by $a \in (\mathbb{Z}_p)^\times$ (not the identity) with $\text{ord}(a) = k$. Lagrange's theorem states this must divide the order of the group. Therefore, for some integer n, we have

$$a^{p-1} = a^{kn} = \left(a^k\right)^n = 1 \mod p.$$

Proof using binomial theorem. We show equivalently that $a^p = a \mod p$. Taking the binomial theorem modulo p yields

$$(a+1)^p = \sum_{k=0}^{p} C(p,k) a^k = a^p + 1 \mod p,$$

since p divides every $C(p, k)$ whenever $1 \leq k \leq p-1$. We next induct on the integer a; i.e.,

[2] A proof will be given in part (c).

suppose the result holds for a (the base case is trivial). Then

$$\begin{aligned}(a+1)^p &= a^p + 1 \mod p && \text{(binomial theorem)}\\ &= a + 1 \mod p && \text{(inductive hypothesis)},\end{aligned}$$

which shows $a^p = a \mod p$.

(c) We first remark that Bézout's identity follows directly from the Euclidean algorithm, which shows that we can iterate division plus remainder,

$$\begin{aligned} b &= q_1 a + r_1 \\ a &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} \\ r_{n-2} &= q_n r_{n-1} + \underbrace{r_n}_{=0}, \end{aligned}$$

such that the process terminates (the r's are strictly decreasing and non-negative) with $r_{n-1} = \gcd(a, b)$. Writing the algorithm in reverse, and plugging in the k-th step to the $(k-1)$-th step, we find $ax + by = \gcd(a, b)$, which proves Bézout's identity.

We next encrypt the secret message M by computing the ciphertext,

$$C = M^e \mod p.$$

From Bézout's identity, we can find some integers d and k such that

$$de - k(p-1)(q-1) = 1,$$

which shows that $de = 1 \mod p$. Decrypting the ciphertext yields

$$C^e = M^{de} = M^{1+k(p-1)(q-1)} = M\big(M^k\big)^{(p-1)(q-1)} \mod N.$$

Now using Fermat's little theorem, we have

$$\Big[\big(M^k\big)^{(p-1)}\Big]^{(q-1)} = (1+nq) \qquad \text{and} \qquad \Big[\big(M^k\big)^{(q-1)}\Big]^{(p-1)} = (1+mp),$$

for some integers n and m. But both left-hand-sides are equal, which implies that $nq = mp$. Hence n must be some multiple of p, and m some multiple of q. This justifies the equality

$M^{(p-1)(q-1)} = 1 \mod N$ (note here, the modulus is not a prime).[3] Therefore, decryption just gives back the plaintext,

$$C^e = M^{de} = M \mod N,$$

as desired.

4 Group Characters and Number Theory

Rearranging and factoring, one finds

$$r_1^2 = r_2^2 \mod p \implies r_1^2 - r_2^2 = (r_1 - r_2)(r_1 + r_2) = 0 \mod p \implies r_1 = \pm r_2 \mod p. \quad (3)$$

Furthermore, $r \neq r \mod p$, which can be seen by rewriting all the elements greater than $(p-1)/2$ (p is an odd prime) in an equivalent form (modulo p),

$$\left\{1, 2, \ldots, \frac{p-1}{2} - 1, \frac{p-1}{2}, \underbrace{\frac{p-1}{2} + 1, \ldots, p-1}_{\text{subtract } p \text{ from these}}\right\} = \left\{1, 2, \ldots, \frac{p-1}{2}, -\left(\frac{p-1}{2}\right), \ldots, -2, -1\right\}.$$

Clearly $(\pm r)$ both square to the same quadratic residue (mod p), and (3) shows that any quadratic residue is only the square of plus or minus a single group element. Hence, exactly half of the elements of $(\mathbb{Z}_p)^\times$ are quadratic residues.

If we define the Legendre symbol as

$$\left(\frac{a}{p}\right) \stackrel{\text{def}}{=} \begin{cases} 0, & a = 0 \\ 1, & a \text{ is a quadratic residue (mod } p) \\ -1, & a \text{ is not a quadratic residue (mod } p), \end{cases} \quad (4)$$

then for any $a, b \in (\mathbb{Z}_p)^\times$,

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right). \quad (5)$$

Proof 1. Whenever a or b is zero, ab is also zero. If both $a, b \in Q$ (i.e., are quadratic residues), then $a = r_1^2 \mod p$ and $b = r_2^2 \mod p$, so that $ab = (r_1 r_2)^2 \mod p$, which shows $ab \in Q$. Note next that if $a = r^2 \mod p$, then $a^{-1} \in Q$. Using Fermat's little theorem, we can write

$$a^{-1} = a^{p-2} = \left(r^{p-2}\right)^2 \mod p.$$

[3] This in fact is a special case of Euler's theorem (one of them at least).

We can use this to show that if $a \in Q$ and $b \notin Q$, then $ab \notin Q$ since, if it were,

$$ab = r^2 \mod p \implies b = a^{-1}r^2 = \left(r'\right)^2 \mod p,$$

which would yield a contradiction since the product of two quadratic residues is a quadratic residue, whereas we assumed $b \notin Q$. To show that if $a, b \notin Q$, then $ab \in Q$, simply note that $Q \sqcup bQ = \mathbb{Z}_p$.[4] Left multiplying by a yields $aQ \cup abQ = \mathbb{Z}_p$, by group closure. Since the aQ gives the set of non-residues, it must be that $abQ = Q$.[5]

Proof 2. Alternatively, we can show that $a^{(p-1)/2} \mod p$ behaves identically to (4) and then use this to verify (5). The $a = 0$ case is trivial. Making use of Fermat's little theorem,

$$\begin{aligned} a \in Q &\implies a^{\frac{p-1}{2}} = \left(r^2\right)^{\frac{p-1}{2}} = r^{p-1} = 1 \mod p \\ a \notin Q &\implies a^{\frac{p-1}{2}} = -1 \mod p, \end{aligned}$$

where in the last equality we used (3). It then follows immediately that

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \mod p = (ab)^{\frac{p-1}{2}} \mod p = \left(\frac{ab}{p}\right).$$

Equation (5) shows that the Legendre symbol forms a one-dimensional representation of $(\mathbb{Z}_p)^\times$. Let Q^+ and Q^- denote the sets of elements with Legendre symbol equal to ± 1, respectively. These partition $(\mathbb{Z}_p)^\times$ so that $|Q^+| + |Q^-| = |\mathbb{Z}_p|$. Using this representation and the trivial representation in the orthogonality theorem gives the additional equation $(+1)|Q^+| + (-1)|Q^-| = 0$, which shows that $|Q^+| = |Q^-| = \frac{p-1}{2}$, as desired.

5 Constructing the Character Table of S_4

The character table is provided in the problem.

	Typical element and size				
	(1)	(12)	(123)	(1234)	(12)(34)
Irrep	1	6	8	6	3
A_1	1	1	1	1	1
A_2	1	-1	1	-1	1
E	2	0	-1	0	2
T_1	3	1	0	-1	-1
T_2	3	-1	0	1	-1

[4] The $\sqcup$ denotes the disjoint union. These two sets form a partition of $\mathbb{Z}_p$.

[5] Although it is not necessary for our purposes, the set Q in fact forms a normal subgroup of $(\mathbb{Z}_p)^\times$. What we have done above amount to working out the multiplication table for the quotient group $\mathbb{Z}_p/Q$.

(a) The number of cycles with a given cycle structure is worked out in section 14.1 of the textbook. There it is also shown that cycles with the same cycle structure belong to the same conjugacy class, and that conjugacy classes are in one-to-one correspondence with the number of irreducible representations. The number of cycles in each conjugacy class are[6]

$$\begin{aligned}
(*) &\longrightarrow 0!\, C(4,0) = 1 \\
(**) &\longrightarrow 1!\, C(4,2) = 6 \\
(***) &\longrightarrow 2!\, C(4,3) = 8 \\
(****) &\longrightarrow 3!\, C(4,4) = 6 \\
(**)(**) &\longrightarrow \tfrac{1}{2}\, C(4,2) = 3.
\end{aligned}$$

Now we also know that $\sum_J (\dim J)^2 = |S_4| = 24$, where J labels different irreducible representations. Or, written in terms of dimensions and multiplicities, $\sum_d n_d d^2 = 24$. However, we know there must be five irreducible representations, since there are five conjugacy classes of S_4. Therefore we must solve $\sum_d n_d d^2 = 24$ subject to $\sum_d n_d = 5$. One can simply check all possibilities to find the unique solution is given by $n_1 = n_3 = 2$, $n_2 = 1$, and $n_4 = n_5 = 0$. Note that this gives us the first column of the character table.

(b) The first row corresponds to the trivial representation; hence all the characters are equal to one. Since, for any $\sigma, \tau \in S_4$,

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau),$$

this provides a one-dimensional representation of the group, where the representation "matrices" (one-by-one) are just ± 1, corresponding to the sign of the permutation. This is shown in the second row of the character table.

(c) To determine the remaining three rows of the table, consider the natural representation of S_4,

$$(*) \longrightarrow \begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix} \qquad (**) \longrightarrow \begin{pmatrix} 0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix} \qquad (***) \longrightarrow \begin{pmatrix} 0&0&1&0\\1&0&0&0\\0&1&0&0\\0&0&0&1 \end{pmatrix}$$

$$(****) \longrightarrow \begin{pmatrix} 0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0 \end{pmatrix} \qquad (**)(**) \longrightarrow \begin{pmatrix} 0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0 \end{pmatrix}.$$

The long arrows in the expression above denote selection of one matrix representative from each conjugacy class in the natural representation. The characters (trace of the matrices above) are easily computed to be $\{4, 2, 1, 0, 0\}$. Now, we are told that the one dimensional vector space spanned by sets of the form $\{a, a, a, a\}$ (call it W) is invariant under the permutation group, and hence transforms like A_1. We can then decompose the full vector space as $V = W \oplus W^\perp$. One can easily verify that the natural representation restricted to $W^\perp$ is the irreducible

[6] Notation: $C(n,k) = \binom{n}{k} = \frac{n!}{k!(n-k)!}$.

representation T_1. We can then compute the characters using

$$\chi_{\text{nat.}} = \chi_{A_1 \oplus T_1} = \chi_{A_1} + \chi_{T_1} \implies \chi_{T_1} = \chi_{\text{nat.}} - \chi_{A_1} = \{3, 1, 0, -1, -1\}.$$

This gives us the fourth row in the character table. This row can also be round in a more geometric fashion. Using a basis in which the origin resides at the center of a tetrahedron, the x axis is parallel to the edge connecting vertices 1 and 2, and the z axis intersects the apex, we have

$$(\,) \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \implies \chi = 3$$

$$(12) \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \implies \chi = 1 \qquad \text{(inversion along } y\text{)}$$

$$(123) \longrightarrow \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} & 0 \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} \implies \chi = 0 \qquad \text{(rotate by } 2\pi/3 \text{ around } z\text{)}.$$

To find the matrix for (12)(34) in the natural representation, we can instead use a tetrahedron inscribed in a cube, as in figure 1, and rotate around the z axis (vertical) by π.[7] This yields

$$(12)(34) \longrightarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \implies \chi = -1.$$

To calculate the final character, choose the representative 4-cycle (1423) which, again in figure 1, corresponds to a $\pi/2$ rotation around the z axis and then an inversion along the z axis (the vertical).

$$(1423) \longrightarrow \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \implies \chi = -1.$$

These characters agree with our previous calculation, as expected.

(d) Lastly, the remaining two rows of the character table can be found using the orthogonality relation (equation 14.22 in the textbook),

$$\sum_i d_i \left(\chi_i^J\right)^* \chi_i^K = |G| \delta^{JK}, \tag{6}$$

[7] Although this uses a different basis, we are only interested in calculating characters, which are class functions and therefore basis independent. Therefore, we are free to use any basis we choose.

where d_i is the size of the corresponding conjugacy class. For each of the remaining irreducible representations, equation (6) yields four equations in four unknowns which can be solved easily. Using (6), the system of equations for the characters of the irreducible representation E, for example, is $(J = E)$

$$\begin{aligned} 2 + 6e_2 + 8e_3 + 6e_4 + 3e_5 &= 0 && (K = A_1) \\ 2 - 6e_2 + 8e_3 - 6e_4 + 3e_5 &= 0 && (K = A_2) \\ 6 + 6e_2 - 6e_4 - 3e_5 &= 0 && (K = T_1) \\ 4 + 6e_2^2 + 8e_3^2 + 6e_4^2 + 3e_5^2 &= 24 && (K = E). \end{aligned}$$

We also know however that $\sum_i d_i = 5$ and that characters for the symmetric group take integer values.[8] After some scratch work, one finds the only possible solutions are $e_2 = e_4 = 0$, $e_3 = -1$, and $e_5 = 2$. The procedure for finding the characters of T_2 is analogous.

Alternatively, for the irreducible representation T_2, we can compose the representations A_2 and T_1 since

$$(\mathrm{sgn}(\sigma)D(\sigma))(\mathrm{sgn}(\tau)D(\tau)) = \mathrm{sgn}(\sigma\tau)D(\sigma\tau);$$

i.e., $\mathrm{sgn}(\,\cdot\,)D(\,\cdot\,)$ satisfies the homomorphism property. This amounts to an element-wise multiplication of the rows for A_2 and T_1 in the character table which gives the characters for T_2.

[8] Note, this is not true generally (i.e., for representations of arbitrary groups). Proving that characters for S_n take only integer values is non-trivial. See, for example, https://mathoverflow.net/questions/10635/why-are-the-characters-of-the-symmetric-group-integer-valued.