1) Group-Theory in theory: Let G be any group.

a) The subset $Z(G)$ of G consisting of those $g \in G$ that commute with all other elements of the group is called the *center* of the group. Show that $Z(G)$ is a subgroup of G.

b) If g is an element of G, the set $C_G(g)$ of elements of G that commute with g is called the *centeralizer* of g in G. Show that it is a subgroup of G.

c) If H is a subgroup, the set of elements of G that commute with all elements of H is the *centralizer* $C_G(H)$ of H in G. Show that it is a subgroup of G.

d) If H is a subgroup, the set $N_G(H) \subset G$ consisting of those g such that $g^{-1}Hg = H$ is called the *normalizer* of H in G. Show that $N_G(H)$ is a subgroup of G, and that H is a normal subgroup of $N_G(H)$.

2) Group Theory in practice:

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

i) Show that D_n has 2n elements. (Hint: they can all be written as a^m, or ba^m.)

ii) Work out the group multiplication table for D_3.

(b) Consider the permutations

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

(i) Express them in cycle notation.

(ii) Determine whether they correspond to even or odd permutations.

(iii) Determine the *order* of these permutations (*i.e.* the smallest number of powers of them needed to arrive at the identity permutation).

(iv) Determine the *order* of the permutation that in cycle notation reads $(\, a_1 a_2 \cdots a_{2r} \,)\,(\, b_1 b_2 \cdots b_r \,)$.

(c) The *tetrahedral group* T is the group of rotations that takes a regular tetrahedron into itself. (Note that a regular tetrahedron can be inscribed in a cube, the tetrahedron's edges being six of the twelve face-diagonals of the cube.) Show that T is generated bt $\{b, c\}$ with $b^2 = c^3 = (bc)^3 = e$, where b is a 2-fold rotation about the x-axis (*i.e.* an axis perpendicular to a cube face and running through a particular opposing pair of cube faces) and c is a 3-fold rotation about one of the cube diagonals.

3) An application of Group thery to Cryptography: The *RSA algorithm*, patented by Rivest, Shamir and Adelman in 1978 and now in the public domain, was the first sucessful *public key* cryptosystem. All prior encryption methods had the vulnerability that a secret *key* had to be exchanged between the two communicating parties (traditionally called Alice

and Bob). With a public key system, knowing the recipe for encoding a mesage gives one no help in decoding it, so the encoding instruction can be made public. The existence of such systems is what makes internet commerce possible. The mathematical foundation of the RSA algorithm is a theorem in number theory discovered by Pierre de Fermat in the 1600's.

a) Show that the set of powers a^n of an element $a \in G$ form a subgroup.

b) Let p be a prime number. Show that the integers $\{1, 2, \ldots, p-1\}$ form a group $(\mathbb{Z}_p)^\times$ of order $(p-1)$ under multiplication modulo p. Hence, by the use of Lagrange's theorem, prove *Fermat's little theorem* that, for any prime p and integer a we have $a^{p-1} = 1, \bmod p$. (Fermat proved that $a^p = a, \bmod p$ by using the binomial theorem. Try this!)

c) Now use Fermat's theorem from part b) to establish the mathematical identity underlying the RSA algorithm: Let p, q be prime and $N = pq$. First use Euclid's algorithm for the highest common factor (also known as the greatest common divisor) of two numbers to show that if the integer e is co-prime to[1] $(p-1)(q-1)$, then there is an integer d such that

$$de = 1, \bmod (p-1)(q-1).$$

Then show that if we encrypt a number M representing a message by computing

$$C = M^e, \bmod N,$$

we can recover the original M by computing

$$M = C^d, \bmod N.$$

The numbers e and N can be made known to the public, but it is hard to find the secret decoding key, d, unless the factors p and q of N are known. The powers of M and C can be computed quickly by using the same trick that makes fast Fourier transforms work.

4) Group characters and number theory: An integer a is said to be a *quadratic residue* mod p if there is an r such that $a = r^2 \pmod p$. Let p be an odd prime. Show that if $r_1^2 = r_2^2 \pmod p$ then $r_1 = \pm r_2 \pmod p$, and that $r \neq -r \pmod p$. Deduce that exactly *one half* of the $p-1$ non-zero elements of $\mathbb{Z}_p$ are quadratic residues.

Now let $\left(\frac{a}{p}\right)$ be the *Legendre symbol*

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

Show that

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right),$$

[1] Has no factors in common with.

and so the Legendre symbol forms a one-dimensional representation of the multiplicative group $(\mathbb{Z}_p)^\times$. Use this fact together with the character orthogonality theorem to give an alternative proof that precisely half the $p-1$ elements of $(\mathbb{Z}_p)^\times$ are quadratic residues.

5) Constructing the character table of S_4:

(a) By considering the possible forms of its cycle notation, determine the number of elements in each conjugacy class of the permutation group S_4 and show that it has five irreducible representations (irreps). Explain why they must consist of two 3-dimensional, one 2-dimensional and two 1-dimensional irreps.

(b) By considering the odd and even permutations in the group, establish the characters of the two 1-dimensional irreps.

(c) Construct a natural representation of S_4 in terms of 4-by-4 matrices based on a set of four objects $\{a, b, c, d\}$, and, by selecting one example of a permutation from each conjugacy class, show that this natural representation has characters $\{4, 2, 1, 0, 0\}$. The 1-dimensional vector space spanned by sets of the form $\{a, a, a, a\}$ is invariant under the permutation group, and hence transforms according to the trivial irrep A_1. The remaining 3-dimensional subspace is irreducible; use this and the characters deduced above to establish the characters of one of the 3-dimensional irreps T_1.

(d) Complete the character table by making use of the character orthogonality theorem, and check the summation rule for each irrep. You should obtain the table

	Typical element and class 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