

CHAPTER 11

Application to Counting

© W W L Chen, 1991, 1993, 2013.

This chapter is available free to all individuals,
on the understanding that it is not to be used for financial gain,
and may be downloaded and/or photocopied,
with or without permission from the author.

However, this document may not be kept on any information storage and retrieval system
without permission from the author,
unless such system is not accessible to any individuals other than its owners.

11.1. Group Actions

We start by looking at two simple examples.

EXAMPLES. (1) Suppose that we have four beads of different colours to put in a ring. In how many different ways can this be achieved? Suppose that the ring has four positions, and that the beads are of colours yellow (Y), green (G), red (R) and blue (B). Then the following two pictures appear to represent two such ways.

$$\begin{array}{ccc} R & \cdots & G \\ \vdots & & \vdots \\ B & \cdots & Y \end{array} \qquad \begin{array}{ccc} R & \cdots & B \\ \vdots & & \vdots \\ G & \cdots & Y \end{array}$$

Indeed, we may suspect that there may be $4! = 24$ different ways of doing this. However, note that either picture can be obtained from the other by a flip and a rotation. In fact, the following eight pictures all represent the same arrangement of the four beads.

$$\begin{array}{cccc} \begin{array}{ccc} R & \cdots & G \\ \vdots & & \vdots \\ B & \cdots & Y \\ [1] \end{array} & \begin{array}{ccc} G & \cdots & Y \\ \vdots & & \vdots \\ R & \cdots & B \\ [2] \end{array} & \begin{array}{ccc} Y & \cdots & B \\ \vdots & & \vdots \\ G & \cdots & R \\ [3] \end{array} & \begin{array}{ccc} B & \cdots & R \\ \vdots & & \vdots \\ Y & \cdots & G \\ [4] \end{array} \\ \\ \begin{array}{ccc} G & \cdots & R \\ \vdots & & \vdots \\ Y & \cdots & B \\ [5] \end{array} & \begin{array}{ccc} R & \cdots & B \\ \vdots & & \vdots \\ G & \cdots & Y \\ [6] \end{array} & \begin{array}{ccc} B & \cdots & Y \\ \vdots & & \vdots \\ R & \cdots & G \\ [7] \end{array} & \begin{array}{ccc} Y & \cdots & G \\ \vdots & & \vdots \\ B & \cdots & R \\ [8] \end{array} \end{array}$$

Indeed, if we associate Y, G, R, B with $1, 2, 3, 4$ respectively, then each of the above eight pictures is obtained from picture [1] by applying the elements (3.2) of the group D_4 . It follows that of the 24 different ways, each one is essentially the same as 7 others, so that there are essentially only $24/8 = 3$ different ways. Note here that the group D_4 plays an important role.

(2) Suppose that we have four different people to sit in a circle. In how many different ways can this be achieved? Suppose that the four people are Yasmin (Y), George (G), Robert (R) and Bianca (B). Let us use the pictures in the previous example. Then it is clear that while pictures [1]–[4] represent essentially the same way, pictures [1] and [5] now represent different ways, unless they are all prepared to sit on the ceiling. It now follows that of the 24 different ways, each one is essentially the same as 3 others, so that there are essentially only $24/4 = 6$ different ways. Note here that the subgroup $\{i, \rho, \rho^2, \rho^3\}$ of D_4 , where $\rho = (1\ 2\ 3\ 4)$, plays an important role.

We next consider a somewhat more complicated problem.

EXAMPLE. Suppose that we have two red beads and two green beads to put in a ring. In how many different ways can this be achieved? The following two pictures appear to represent two such ways.

$$\begin{array}{ccc} R & \cdots & G \\ \vdots & [A] & \vdots \\ G & \cdots & R \end{array} \qquad \begin{array}{ccc} R & \cdots & R \\ \vdots & [B] & \vdots \\ G & \cdots & G \end{array}$$

Indeed, we may suspect that there may be $\binom{4}{2} = 6$ different ways of doing this. After all, once we have chosen two places for the red beads, the remaining two places go to the green beads. Now let us apply each permutation in D_4 to the picture [A]. Then we get the following arrangements.

$$\begin{array}{cccc} \begin{array}{ccc} R & \cdots & G \\ \vdots & [A] & \vdots \\ G & \cdots & R \\ [1] \end{array} & \begin{array}{ccc} G & \cdots & R \\ \vdots & [A] & \vdots \\ R & \cdots & G \\ [2] \end{array} & \begin{array}{ccc} R & \cdots & G \\ \vdots & [A] & \vdots \\ G & \cdots & R \\ [3] \end{array} & \begin{array}{ccc} G & \cdots & R \\ \vdots & [A] & \vdots \\ R & \cdots & G \\ [4] \end{array} \\ & \begin{array}{ccc} G & \cdots & R \\ \vdots & [A] & \vdots \\ R & \cdots & G \\ [5] \end{array} & \begin{array}{ccc} R & \cdots & G \\ \vdots & [A] & \vdots \\ G & \cdots & R \\ [6] \end{array} & \begin{array}{ccc} G & \cdots & R \\ \vdots & [A] & \vdots \\ R & \cdots & G \\ [7] \end{array} & \begin{array}{ccc} R & \cdots & G \\ \vdots & [A] & \vdots \\ G & \cdots & R \\ [8] \end{array} \end{array}$$

These fall into two types. Next let us apply each permutation in D_4 to the picture [B]. Then we get the following arrangements.

$$\begin{array}{cccc} \begin{array}{ccc} R & \cdots & R \\ \vdots & [B] & \vdots \\ G & \cdots & G \\ [1] \end{array} & \begin{array}{ccc} R & \cdots & G \\ \vdots & [B] & \vdots \\ R & \cdots & G \\ [2] \end{array} & \begin{array}{ccc} G & \cdots & G \\ \vdots & [B] & \vdots \\ R & \cdots & R \\ [3] \end{array} & \begin{array}{ccc} G & \cdots & R \\ \vdots & [B] & \vdots \\ G & \cdots & R \\ [4] \end{array} \\ & \begin{array}{ccc} R & \cdots & R \\ \vdots & [B] & \vdots \\ G & \cdots & G \\ [5] \end{array} & \begin{array}{ccc} R & \cdots & G \\ \vdots & [B] & \vdots \\ R & \cdots & G \\ [6] \end{array} & \begin{array}{ccc} G & \cdots & G \\ \vdots & [B] & \vdots \\ R & \cdots & R \\ [7] \end{array} & \begin{array}{ccc} G & \cdots & R \\ \vdots & [B] & \vdots \\ G & \cdots & R \\ [8] \end{array} \end{array}$$

These now fall into four types. We conclude that of the 6 different ways, 4 are essentially the same, while the remaining 2 are also essentially the same.

Note the following point which is common to all three examples. We have a set X of configurations, and they are acted on by a group. Our idea is to put essentially similar things into the same collection, and to determine the number of different collections.

DEFINITION. Suppose that X is a non-empty set, and that G is a group with identity element e . We say that G acts on X if the following conditions are satisfied:

- (A1) For every $x \in X$ and $g \in G$, $xg \in X$.
- (A2) For every $x \in X$ and $g, h \in G$, $(xg)h = x(gh)$.
- (A3) For every $x \in X$, $xe = x$.

REMARK. A good way to interpret this is to think of the elements of X as objects and the elements of G as functions.

DEFINITION. Suppose that the group G acts on the non-empty set X . For every $x \in X$, the orbit of x is defined by

$$\mathcal{O}(x) = \{xg : g \in G\}.$$

THEOREM 11.1. Suppose that the group G acts on the non-empty set X . Then

- (i) for every $x, y \in X$, either $\mathcal{O}(x) = \mathcal{O}(y)$ or $\mathcal{O}(x) \cap \mathcal{O}(y) = \emptyset$; and
- (ii) the distinct orbits of G form a partition of X .

PROOF. Define a relation $\sim$ on the set X as follows. For every $x, y \in X$, we write $x \sim y$ whenever there exists $g \in G$ such that $y = xg$. Clearly $\sim$ is reflexive, in view of (A3). On the other hand, for every $x, y \in X$, if $y = xg$, then in view of (A2) and (A3), we have

$$x = xe = x(gg^{-1}) = (xg)g^{-1} = yg^{-1},$$

so that $\sim$ is symmetric. Finally, for every $x, y, z \in X$, if $y = xg$ and $z = yh$, then in view of (A2), we have $z = (xg)h = x(gh)$, so that $\sim$ is transitive. It follows that $\sim$ is an equivalence relation on X . To complete the proof, it remains to show that for every $x \in X$, the equivalence class $[x]$ of x is $\mathcal{O}(x)$. Clearly

$$[x] = \{y \in X : x \sim y\} = \{y \in X : y = xg \text{ for some } g \in G\} = \{xg : g \in G\} = \mathcal{O}(x),$$

as required. $\circ$

DEFINITION. Suppose that the group G acts on the non-empty set X . For every $x \in X$, the stabilizer of x is defined by

$$\mathcal{S}(x) = \{g \in G : xg = x\}.$$

THEOREM 11.2. Suppose that the group G acts on the non-empty set X . Then for every $x \in X$,

- (i) $\mathcal{S}(x)$ is a subgroup of G ; and
- (ii) $|\mathcal{O}(x)|$ is equal to the number of left cosets of $\mathcal{S}(x)$ in G .

PROOF. (i) Clearly $e \in \mathcal{S}(x)$ in view of (A3), so that $\mathcal{S}(x)$ is non-empty. Suppose now that $g, h \in \mathcal{S}(x)$. Then $xg = x$ and $xh = x$. Furthermore, in view of (A2) and (A3), we have

$$x = xe = x(hh^{-1}) = (xh)h^{-1} = xh^{-1}.$$

It follows from (A2) that $x(gh^{-1}) = (xg)h^{-1} = xh^{-1} = x$, so that $gh^{-1} \in \mathcal{S}(x)$. Hence $\mathcal{S}(x)$ is a subgroup of G in view of Theorem 1.5.

(ii) Let $\mathcal{T}$ denote the collection of all left cosets of $\mathcal{S}(x)$ in G . Define a function $\phi : \mathcal{T} \rightarrow \mathcal{O}(x)$ as follows. Every coset in $\mathcal{T}$ is of the form $g\mathcal{S}(x)$, where $g \in G$. We now write $(g\mathcal{S}(x))\phi = xg^{-1}$. To show that ϕ is well defined, note that if $g, h \in G$ and $g\mathcal{S}(x) = h\mathcal{S}(x)$, then $h^{-1}g\mathcal{S}(x) = \mathcal{S}(x)$, so that $h^{-1}g \in \mathcal{S}(x)$. It follows that $x(h^{-1}g) = x$, so that $xh^{-1} = xg^{-1}$. It now remains to show that ϕ is one-to-one and onto. To show that ϕ is one-to-one, suppose that $g, h \in G$ and $xg^{-1} = xh^{-1}$. Then $x(h^{-1}g) = x$, so that $h^{-1}g \in \mathcal{S}(x)$, whence $g\mathcal{S}(x) = h\mathcal{S}(x)$. To show that ϕ is onto, simply note that for every $xg \in \mathcal{O}(x)$, we have $xg = (g^{-1}\mathcal{S}(x))\phi$. $\circ$

EXAMPLES. (1) How many different 9-letter words can we form from the letters of *ALGEBRAIC*? To solve this problem, let X be the collection of all 9-letter words. The group S_9 acts on X by permuting the letters of any word in X . For example,

$$(ECONOMICS)(1\ 9\ 8\ 5\ 7\ 4\ 6\ 3\ 2) = COMICNOSE.$$

Now let $x = \text{ALGEBRAIC}$. We are interested in $\mathcal{O}(x)$. In view of Theorem 11.2, it remains to study $\mathcal{S}(x)$. Note that $\mathcal{S}(x) = \{i, (1\ 7)\}$. Hence $|\mathcal{O}(x)| = |S_9|/|\mathcal{S}(x)| = 9!/2$.

(2) How many different 12-letter words can we form from the letters of *HOMOMORPHISM*? To solve this problem, let X be the collection of all 12-letter words. The group S_{12} acts on X by permuting the letters of any word in X . Now let $x = \text{HOMOMORPHISM}$. Note that

$$\mathcal{S}(x) = \{\alpha\beta\gamma : \alpha \text{ permutes } 1, 9 \text{ only}; \beta \text{ permutes } 2, 4, 6 \text{ only}; \gamma \text{ permutes } 3, 5, 12 \text{ only}\},$$

so that $|\mathcal{S}(x)| = 2!3!3!$. It follows from Theorem 11.2 that $|\mathcal{O}(x)| = 12!/2!3!3!$.

11.2. Burnside's Theorem

DEFINITION. Suppose that the group G acts on the non-empty set X . For every $g \in G$, let

$$\mathcal{F}(g) = \{x \in X : xg = x\}.$$

REMARKS. (1) Note that $\mathcal{F}(g)$ is the set of all elements in X fixed by g .

(2) Note that $x \in \mathcal{F}(g)$ if and only if $g \in \mathcal{S}(x)$.

In the case of G and X both finite, we have the following interesting result.

THEOREM 11.3 (Burnside). *Suppose that a finite group G acts on a non-empty finite set X . Then the number of different orbits of G is given by*

$$\frac{1}{|G|} \sum_{g \in G} |\mathcal{F}(g)|.$$

PROOF. In view of Theorem 11.1, let $X = \mathcal{O}_1 \cup \dots \cup \mathcal{O}_N$ be the partition of the set X into a union of distinct orbits. Suppose that $\mathcal{O}$ is one such orbit, and suppose that $\mathcal{O} = \{x_1, \dots, x_k\}$. Then $|\mathcal{O}| = k$. Furthermore, for every $j = 1, \dots, k$, we have $|\mathcal{O}| = |G|/|\mathcal{S}(x_j)|$ by Theorem 11.2. It follows that

$$|\mathcal{S}(x_1)| + \dots + |\mathcal{S}(x_k)| = \underbrace{\frac{|G|}{|\mathcal{O}|} + \dots + \frac{|G|}{|\mathcal{O}|}}_k = |G|,$$

so that

$$(11.1) \quad \sum_{x \in X} |\mathcal{S}(x)| = N|G|.$$

Next, note that

$$(11.2) \quad \sum_{x \in X} |\mathcal{S}(x)| = \sum_{g \in G} |\mathcal{F}(g)|.$$

To see this, note that since $x \in \mathcal{F}(g)$ if and only if $g \in \mathcal{S}(x)$, it follows that every such pair (x, g) contributes equally to both sides of (11.2). The result now follows on combining (11.1) and (11.2). $\circ$

EXAMPLE. We return to the third example in Section 11.1 concerning two red beads and two green beads. Let X denote the set of $\binom{4}{2}$ ways of putting two red beads and two green beads at the corners of a square. The set X is acted on by the group D_4 . The number of essentially different ways of putting these beads in a ring is equal to the number N of orbits. By Burnside's theorem,

$$N = \frac{1}{|D_4|} \sum_{g \in D_4} |\mathcal{F}(g)|.$$

We therefore need to investigate $\mathcal{F}(g)$ for every $g \in D_4$. Note that the elements of X are described by the following pictures.

$$\begin{array}{ccc} R & \dots & G \\ \vdots & & \vdots \\ G & \dots & R \\ & [a] & \end{array} \quad \begin{array}{ccc} R & \dots & R \\ \vdots & & \vdots \\ G & \dots & G \\ & [b] & \end{array} \quad \begin{array}{ccc} R & \dots & G \\ \vdots & & \vdots \\ R & \dots & G \\ & [c] & \end{array}$$

$$\begin{array}{ccc} G & \dots & R \\ \vdots & & \vdots \\ R & \dots & G \\ & [d] & \end{array} \quad \begin{array}{ccc} G & \dots & G \\ \vdots & & \vdots \\ R & \dots & R \\ & [e] & \end{array} \quad \begin{array}{ccc} G & \dots & R \\ \vdots & & \vdots \\ G & \dots & R \\ & [f] & \end{array}$$

We can now check, in the notation of Section 3.3 that

- i fixes $[a]$ – $[f]$;
- $\rho = (1\ 2\ 3\ 4)$ fixes no element;
- $\rho^2 = (1\ 3)(2\ 4)$ fixes $[a]$ and $[d]$;
- $\rho^3 = (1\ 4\ 3\ 2)$ fixes no element;
- $\phi_1 = (1\ 4)(2\ 3)$ fixes $[b]$ and $[e]$;
- $\phi_1\rho = (2\ 4)$ fixes $[a]$ and $[d]$;
- $\phi_1\rho^2 = (1\ 2)(3\ 4)$ fixes $[c]$ and $[f]$; and
- $\phi_1\rho^3 = (1\ 3)$ fixes $[a]$ and $[d]$.

It follows that

$$N = \frac{1}{8}(6 + 0 + 2 + 0 + 2 + 2 + 2 + 2) = 2.$$

11.3. Conjugates

DEFINITION. Suppose that G is a group, and that $x, y \in G$. Then y is called a conjugate of x if there exists $g \in G$ such that $y = g^{-1}xg$.

REMARK. Clearly if y is a conjugate of x , then x is a conjugate of y . We therefore sometimes say that x and y are conjugates.

DEFINITION. Suppose that G is a group. For every $x \in G$, the conjugacy class of x is defined by

$$O(x) = \{g^{-1}xg : g \in G\}.$$

REMARK. Think of the element g as some kind of conjugate-producing function.

THEOREM 11.4. *Suppose that G is a group. Then*

- (i) *for every $x, y \in G$, either $O(x) = O(y)$ or $O(x) \cap O(y) = \emptyset$; and*
- (ii) *the distinct sets $O(x)$ of G form a partition of G .*

PROOF. Define a relation $\sim$ on the group G as follows. For every $x, y \in G$, we write $x \sim y$ whenever there exists $g \in G$ such that $y = g^{-1}xg$. Clearly $\sim$ is reflexive, for $x = e^{-1}xe$ for every $x \in G$. On the other hand, for every $x, y \in G$, if $y = g^{-1}xg$, then we have $x = gyg^{-1} = (g^{-1})^{-1}y(g^{-1})$, so that $\sim$ is symmetric. Finally, for every $x, y, z \in G$, if $y = g^{-1}xg$ and $z = h^{-1}yh$, then we have $z = h^{-1}g^{-1}xgh = (gh)^{-1}x(gh)$, so that $\sim$ is transitive. It follows that $\sim$ is an equivalence relation on G . To complete the proof, it remains to show that for every $x \in G$, the equivalence class $[x]$ of x is $O(x)$. Clearly

$$[x] = \{y \in X : x \sim y\} = \{y \in X : y = g^{-1}xg \text{ for some } g \in G\} = \{g^{-1}xg : g \in G\} = O(x),$$

as required. $\bigcirc$

EXAMPLE. Consider the group S_5 . We shall study the conjugacy classes of S_5 . Note first of all that for every $\phi \in S_5$ and every cycle $(a_1 \dots a_k) \in S_5$, we have

$$\phi^{-1}(a_1 \dots a_k)\phi = (a_1\phi \dots a_k\phi).$$

It follows that all permutations in S_5 having the same cycle structure are conjugates of each other, and that permutations in S_5 having different cycle structures are not conjugates of each other. This means that the number of elements in a conjugacy class in S_5 is the number of different permutations having the same cycle structure. We can therefore summarize our argument in the following table.

Cycle structure	Size of conjugacy class
i	1
$(a \ b)$	$\binom{5}{2} = 10$
$(a \ b \ c)$	$\binom{5}{3}2 = 20$
$(a \ b \ c \ d)$	$\binom{5}{4}3! = 30$
$(a \ b \ c \ d \ e)$	$\binom{5}{5}4! = 24$
$(a \ b)(c \ d)$	$\binom{5}{2}\binom{3}{2}/2 = 15$
$(a \ b)(c \ d \ e)$	$\binom{5}{3}2 = 20$

DEFINITION. Suppose that G is a group. For every $x \in G$, the centralizer of x is defined by

$$C(x) = \{g \in G : xg = gx\}.$$

REMARK. Note that $g \in C(x)$ if and only if $g^{-1}xg = x$.

THEOREM 11.5. *Suppose that G is a group. Then for every $x \in X$,*

- (i) *$C(x)$ is a subgroup of G ; and*
- (ii) *$|O(x)|$ is equal to the number of left cosets of $C(x)$ in G .*

PROOF. (i) Clearly $e \in C(x)$, so that $C(x)$ is non-empty. Suppose now that $g, h \in C(x)$. Then $xg = gx$ and $xh = hx$. Furthermore, we have $h^{-1}x = xh^{-1}$. It follows that

$$x(gh^{-1}) = (xg)h^{-1} = (gx)h^{-1} = g(xh^{-1}) = g(h^{-1}x) = (gh^{-1})x,$$

so that $gh^{-1} \in C(x)$. Hence $C(x)$ is a subgroup of G in view of Theorem 1.5.

(ii) Let T denote the collection of all left cosets of $C(x)$ in G . Define a function $\phi : T \rightarrow O(x)$ as follows. Every coset in T is of the form $gC(x)$, where $g \in G$. We now write

$$(gC(x))\phi = gxg^{-1} = (g^{-1})^{-1}x(g^{-1}).$$

To show that ϕ is well defined, note that if $g, h \in G$ and $gC(x) = hC(x)$, then $h^{-1}gC(x) = C(x)$, so that $h^{-1}g \in C(x)$. It follows that $x(h^{-1}g) = (h^{-1}g)x$, so that $h x h^{-1} = g x g^{-1}$. It now remains to show that ϕ is one-to-one and onto. To show that ϕ is one-to-one, suppose that $g, h \in G$ and $g x g^{-1} = h x h^{-1}$. Then $x(h^{-1}g) = (h^{-1}g)x$, so that $h^{-1}g \in C(x)$, whence $gC(x) = hC(x)$. To show that ϕ is onto, simply note that for every $g^{-1}xg \in O(x)$, we have $g^{-1}xg = (g^{-1}C(x))\phi$. $\square$

EXAMPLES. (1) The permutation $(1\ 2\ 3)$ has 20 distinct conjugates in S_5 . It therefore follows from Theorem 11.5 that $|C((1\ 2\ 3))| = 5!/20 = 6$. Naturally the permutations

$$i, (1\ 2\ 3), (4\ 5) \in C((1\ 2\ 3)).$$

Taking powers and products, we see that

$$(1\ 3\ 2), (1\ 2\ 3)(4\ 5), (1\ 3\ 2)(4\ 5) \in C((1\ 2\ 3)).$$

It follows that

$$C((1\ 2\ 3)) = \{i, (1\ 2\ 3), (1\ 3\ 2), (4\ 5), (1\ 2\ 3)(4\ 5), (1\ 3\ 2)(4\ 5)\}.$$

(2) We would like to find the number of different conjugates of $(1\ 2\ 3\ 4\ 5)$ in A_5 . Let us first investigate $C((1\ 2\ 3\ 4\ 5))$ in S_5 . Clearly, if we write $\phi = (1\ 2\ 3\ 4\ 5)$, then

$$i, \phi, \phi^2, \phi^3, \phi^4 \in C((1\ 2\ 3\ 4\ 5)).$$

Next, recall that $(1\ 2\ 3\ 4\ 5)$ has 24 conjugates in S_5 . It follows from Theorem 11.5 that $C((1\ 2\ 3\ 4\ 5))$ has $5!/24 = 5$ elements in S_5 . These must be the 5 elements listed. Hence $|C((1\ 2\ 3\ 4\ 5))| = 5$ in A_5 . It follows again from Theorem 11.5 that $(1\ 2\ 3\ 4\ 5)$ has $|A_5|/5 = 60/5 = 12$ different conjugates in A_5 .

11.4. The Class Equation

We are interested in determining whether a given group G has non-trivial normal subgroups N , as the factor groups G/N are useful in the study of G .

DEFINITION. Suppose that G is a group. Then the centre of the group G is defined by

$$Z(G) = \{g \in G : xg = gx \text{ for every } x \in G\}.$$

In the case of G finite, we have the following interesting result.

PROPOSITION 11.6 (Class equation). *Suppose that G is a finite group, and that $G = O_1 \cup \dots \cup O_k$ represents a partition of G into a union of disjoint conjugacy classes. Then*

$$(11.3) \quad |G| = |Z(G)| + \sum_{\substack{j=1 \\ |O_j| > 1}}^k \frac{|G|}{|C(x_j)|},$$

where, for every $j = 1, \dots, k$ with $|O_j| > 1$, we have $x_j \in O_j$.

PROOF. Clearly $x \in Z(G)$ if and only if $O(x) = \{x\}$. It follows that

$$|G| = |Z(G)| + \sum_{\substack{j=1 \\ |O_j| > 1}}^k |O_j|.$$

The result follows on noting that $|G| = |C(x_j)||O_j|$ for every $j = 1, \dots, k$ and $x_j \in O_j$. $\square$

EXAMPLE. Consider again the group A_5 . The elements have cycle structures i , $(a\ b\ c)$, $(a\ b\ c\ d\ e)$ or $(a\ b)(c\ d)$. We have already shown that $(1\ 2\ 3\ 4\ 5)$ has 12 different conjugates in A_5 . This gives rise to a conjugacy class of 12 elements. On the other hand, it can be shown that $(1\ 2\ 3\ 5\ 4)$ does not belong to this conjugacy class. Arguing as before, we can show that $(1\ 2\ 3\ 5\ 4)$ has 12 different conjugates in A_5 , giving rise to a second conjugacy class of 12 elements. Furthermore, these

two conjugacy classes together contain all the 24 elements in A_5 of the type $(a\ b\ c\ d\ e)$. Next, the centralizer of $(1\ 2\ 3)$ in S_5 contains 6 elements, 3 of which are odd. Hence in A_5 , we have

$$C((1\ 2\ 3)) = \{i, (1\ 2\ 3), (1\ 3\ 2)\}.$$

It follows from Theorem 11.5 that $(1\ 2\ 3)$ has $60/3 = 20$ conjugates in A_5 , giving rise to a conjugacy class of 20 elements. This conjugacy class clearly contains all the 20 elements in A_5 of the type $(a\ b\ c)$. Finally, the element $(1\ 2)(3\ 4)$ has 15 conjugates in S_5 . By Theorem 11.5, its centralizer in S_5 contains $120/15 = 8$ elements. Let $C((1\ 2)(3\ 4))$ denote the centralizer of $(1\ 2)(3\ 4)$ in A_5 . Then $C((1\ 2)(3\ 4))$ is a subgroup of A_5 as well as a subgroup of the centralizer of $(1\ 2)(3\ 4)$ in S_5 . It follows from Lagrange's theorem that $|C((1\ 2)(3\ 4))|$ divides both 60 and 8, so that $|C((1\ 2)(3\ 4))|$ divides 4. If $|C((1\ 2)(3\ 4))|$ is less than 4, then it follows from Theorem 11.5 that $(1\ 2)(3\ 4)$ has more than $60/4 = 15$ conjugates in A_5 , clearly impossible. It follows that $|C((1\ 2)(3\ 4))| = 4$, giving rise to a conjugacy class of 15 elements. We can therefore verify the Class equation:

$$\begin{aligned} |A_5| &= |Z(A_5)| + \frac{|A_5|}{|C((1\ 2\ 3\ 4\ 5))|} + \frac{|A_5|}{|C((1\ 2\ 3\ 5\ 4))|} + \frac{|A_5|}{|C((1\ 2\ 3))|} + \frac{|A_5|}{|C((1\ 2)(3\ 4))|} \\ &= 1 + \frac{60}{5} + \frac{60}{5} + \frac{60}{3} + \frac{60}{4} = 1 + 12 + 12 + 20 + 15 = 60. \end{aligned}$$

EXAMPLE. We can now show that A_5 has no non-trivial normal subgroups. Suppose that N is a normal subgroup of A_5 , and that $x \in N$. Let $y \in O(x)$. Then $y = g^{-1}xg$ for some $g \in A_5$. It follows that for every $h \in A_5$, we have $h^{-1}yh = h^{-1}g^{-1}xgh = (gh)^{-1}x(gh) \in N$. Hence $O(x) \subseteq N$. This means that if a normal subgroup contains an element of a conjugacy class, then it must contain every element of that conjugacy class. Suppose now that N is a normal subgroup of A_5 containing not only the identity element i . Then N must be a union of conjugacy classes in A_5 . This union must contain $O(i)$, a conjugacy class of 1 element. The other four conjugacy classes have 12, 12, 20, 15 elements. Clearly it is impossible to obtain a sum of 1 and a selection of one or more numbers from 12, 12, 20, 15 such that this sum is a proper divisor of 60. It follows that A_5 has no non-trivial normal subgroups.

We conclude this chapter by considering an application of Theorem 11.6 to groups of prime power order.

THEOREM 11.7. *Suppose that G is a group of order p^k , where p is prime and $k \in \mathbb{N}$. Then $|Z(G)| > 1$.*

PROOF. Consider the class equation (11.3). Since both

$$|G| \quad \text{and} \quad \sum_{\substack{j=1 \\ |O_j| > 1}}^k \frac{|G|}{|C(x_j)|}$$

are multiples of p , it follows that $|Z(G)|$ is also a multiple of p . Since $|Z(G)| \geq 1$, it follows that $|Z(G)| > 1$. $\circ$

REMARK. We can now prove that every group of order p^2 , where p is a prime, is abelian. See Problem 17 in Chapter 4.

Problems for Chapter 11

1. Explain clearly, in terms of group action, how many different 24-letter words we can form from the letters of *MOSTPOLITICIANSARECROOKS*.

2. In how many different ways can two red beads and two green beads be placed in the four corners of a rectangular non-square frame?

3. In how many different ways can we move from the origin $(0, 0, 0)$ to the point $(3, 3, 3)$ by moving 1 unit in the positive x -, y - or z -direction at a time?

[Hint: We need to move in each direction precisely 3 units.]

4. Find all the elements of S_4 that commute with $(1\ 2)(3\ 4)$.

5. Write down the class equation for each of the following groups:

(i) S_4

(ii) A_4

(iii) $S_3 \times \mathbb{Z}_2$

6. Show that $(1\ 2\ 3\ 4\ 5)$ and $(1\ 2\ 3\ 5\ 4)$ are not conjugates in A_5 by following the following steps:

(i) Describe the element $\phi^{-1}(1\ 2\ 3\ 4\ 5)\phi$ for any $\phi \in S_5$.

(ii) Determine all $\phi \in S_5$ such that $\phi^{-1}(1\ 2\ 3\ 4\ 5)\phi = (1\ 2\ 3\ 5\ 4)$.

(iii) Show that all the $\phi \in S_5$ in (ii) are odd.

7. Give an example of a group G and subgroups H and K of G such that all of the following conditions are satisfied:

(i) H is normal in G .

(ii) K is a subgroup of H .

(iii) K is not normal in G .