Cambridge University Press
978-1-316-61044-2 - Topics in Graph Automorphisms and Reconstruction
Josef Lauri and Raffaele Scapellato
Excerpt
More information

1

Graphs and Groups: Preliminaries

1.1 Graphs and digraphs

In these chapters a *graph* $G = (V(G), E(G))$ will consist of two disjoint sets: a nonempty set $V = V(G)$ whose elements will be called *vertices* and a set $E = E(G)$ whose elements, called *edges*, will be unordered pairs of distinct elements of V. Unless explicitly stated otherwise, the set of vertices will always be finite. An edge, $\{u, v\}$, $u, v \in V$, is also denoted by uv. Sometimes E is allowed to be a multiset, that is, the same edge can be repeated more than once in E. Such edges are called *multiple edges*. Also, edges uu consisting of a pair of repeated vertices are sometimes allowed; such edges are called *loops*. But unless otherwise stated, it will always be assumed that a graph does not have loops or multiple edges. The *complement* of the graph G, denoted by $\overline{G}$, has the same vertex-set as G, but two distinct vertices are adjacent in the complement if and only if they are not adjacent in G.

The *degree* of a vertex v, denoted by $\deg(v)$, is the number of edges in $E(G)$ to which v belongs. A vertex of degree k is sometimes said to be a *k-vertex*. Two vertices belonging to the same edge are said to be *adjacent*, while a vertex and an edge to which it belongs are said to be *incident*. A loop incident to a vertex v contributes a value of 2 to $\deg(v)$. A graph is said to be *regular* if all of its vertices have the same degree. A regular graph with degree equal to 3 is sometimes called *cubic*. The minimum and maximum degrees of G are denoted by $\delta = \delta(G)$ and $\Delta = \Delta(G)$, respectively.

In general, given any two sets A, B, then $A - B$ will denote their set-theoretical difference, that is, the set consisting of all of the elements that are in A but not in B. Also, a set containing k elements is often said to be a *k-set*.

If S is a set of vertices of a graph G, then $G - S$ will denote the graph obtained by removing S from $V(G)$ and removing from $E(G)$ all edges incident to some vertex in S. If F is a set of edges of G, then $G - F$ will denote the graph whose vertex-set is $V(G)$ and whose edge-set is $E(G) - F$. If $S = \{u\}$ and $F = \{e\}$, we shall, for short, denote $G - S$ and $G - F$ by $G - u$ and $G - e$, respectively.

If S is a subset of the vertices of G, then $G[S]$ will denote the subgraph of G *induced* by S, that is, the subgraph consisting of the vertices in S and all of the edges joining pairs of vertices from S.

An important modification of the foregoing definition of a graph gives what is called a *directed graph*, or *digraph* for short. In a digraph $D = (V(D), A(D))$ the set $A = A(D)$ consists of ordered pairs of vertices from $V = V(D)$ and its elements are called *arcs*. Again, an arc (u, v) is sometimes denoted by uv when it is clear from the context whether we are referring to an arc or an edge. The arc uv is said to be *incident to* v and *incident from* u; the vertex u is said to be *adjacent to* v whereas v is *adjacent from* u. The number of arcs incident from a vertex v is called its *out-degree*, denoted by $\deg_{\text{out}}(v)$, while the number of arcs incident to v is called its *in-degree* and is denoted by $\deg_{\text{in}}(v)$. A digraph is said to be *regular* if all of its vertices have the same out-degree or, equivalently, the same in-degree. Sometimes, when we need to emphasise the fact that a graph is not directed, we say that it is *undirected*.

The number of vertices of a graph G or digraph D is called its *order* and is generally denoted by $n = n(G)$ or $n = n(D)$, while the number of edges or arcs is called its *size* and is denoted by $m = m(G)$ or $m = m(D)$.

A sequence of distinct vertices of a graph, $v_1, v_2, \ldots, v_{k+1}$, and edges $e_1, e_2, \ldots, e_k$ such that each edge $e_i = v_iv_{i+1}$ is called a *path*. If we allow v_1 and v_{k+1}, and only those, to be the same vertex, then we get what is called a *cycle*.

The *length* of a path or a cycle in G is the number of edges in the path or cycle. A path of length k is denoted by P_{k+1} while a cycle of length k is denoted by C_k. The *distance* between two vertices u, v in a connected graph G, denoted by $d(u, v)$, is the length of the shortest path joining u and v. The *diameter* of G is the maximum value attained by $d(u, v)$ as u, v run over $V(G)$, and the *girth* is the length of the shortest cycle.

In these definitions, if we are dealing with a digraph and the $e_i = v_iv_{i+1}$ are arcs, then the path or cycle is called a *directed path* or *directed cycle*, respectively.

Given a digraph D, the *underlying graph* of D is the graph obtained from D by considering each pair in $A(D)$ to be an unordered pair. Given a graph G, the digraph $\overleftrightarrow{G}$ is obtained from G by replacing each edge in $E(G)$ by a pair of oppositely directed arcs. This way, a graph can always be seen as a special case of a digraph.

We adopt the usual convention of representing graphs and digraphs by drawings in which each vertex is shown by a dot, each edge by a curve joining the corresponding pair of dots and each arc (u, v) by a curve with an arrowhead pointing in the direction from u to v.

A number of definitions on graphs and digraphs will be given as they are required. However, several standard graph theoretic terms will be used but not defined in these chapters; these can be found in any of the references [257] or [259].

1.2 Groups

A *permutation group* will be a pair (Γ, Y) where Y is a finite set and Γ is a subgroup of the symmetric group S_Y, that is, the group of all permutations of Y. The stabiliser of an element $y \in Y$ under the action of Γ is denoted by Γ_y while the orbit of y is denoted by $\Gamma(y)$. The *Orbit-Stabiliser Theorem* states that, for any element $y \in Y$,

$$|\Gamma| = |\Gamma(y)| \cdot |\Gamma_y|.$$

If the elements of Y are all in one orbit, then (Γ, Y) is said to be a *transitive permutation group* and Γ is said to act *transitively* on Y. The permutation group Γ is said to act *regularly* on Y if it acts transitively and the stabiliser of any element of Y is trivial. By the Orbit-Stabiliser Theorem, this is equivalent to saying that Γ acts transitively on Y and $|\Gamma| = |Y|$. Also, Γ acts regularly on Y is equivalent to saying that, for any $y_1, y_2 \in Y$, there exists exactly one $\alpha \in \Gamma$ such that $\alpha(y_1) = y_2$.

One important regular action of a permutation group arises as follows. Let Γ be any group, let $Y = \Gamma$ and, for any $\alpha \in \Gamma$, let λ_α be the permutation of Y defined by $\lambda_\alpha(\beta) = \alpha\beta$. Let $L(\Gamma)$ be the set of all permutations λ_α for all $\alpha \in \Gamma$. Then $(L(\Gamma), Y)$ defines a permutation group acting regularly on Y. This is called the *left regular representation* of the group Γ on itself. One can similarly consider the *right regular representation* of the group Γ on itself, and this is denoted by $(R(\Gamma), Y)$.

The following is an important generalisation of the previous definitions. If Γ is a group and $\mathcal{H} \leq \Gamma$, let $Y = \Gamma/\mathcal{H}$ be the set of left cosets of $\mathcal{H}$ in Γ. For any $\alpha \in \Gamma$, let $\lambda_\alpha^{\mathcal{H}}$ be a permutation on Y defined by $\lambda_\alpha^{\mathcal{H}}(\beta\mathcal{H}) = \alpha\beta\mathcal{H}$. Let $L^{\mathcal{H}}(\Gamma)$ be the set of all $\lambda_\alpha^{\mathcal{H}}$ for all $\alpha \in \Gamma$. Then $(L^{\mathcal{H}}(\Gamma), Y)$ defines a permutation group that reduces to the left regular representation of Γ if $\mathcal{H} = \{1\}$.

Two permutation groups $(\Gamma_1, Y_1), (\Gamma_2, Y_2)$ are said to be *equivalent*, denoted by $(\Gamma_1, Y_1) \equiv (\Gamma_2, Y_2)$, if there exists a bijective isomorphism $\phi : \Gamma_1 \to \Gamma_2$ and a bijection $f : Y_1 \to Y_2$ such that, for all $y \in Y_1$ and for all $\alpha \in \Gamma_1$,

$$f(\alpha(x)) = \phi(\alpha)(f(x)).$$

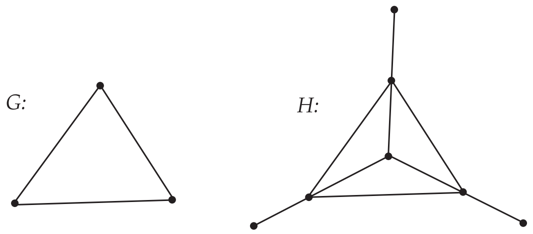

Figure 1.1. Aut(G), Aut(H) are isomorphic but not equivalent

In this case we also say that the action of Γ_1 on Y_1 is equivalent to the action of Γ_2 on Y_2, and sometimes we denote this simply by $\Gamma_1 = \Gamma_2$, when the two sets on which the groups are acting is clear from the context.

Figure 1.1 shows a simple example of two graphs whose automorphism groups (to be defined later in this chapter) are isomorphic as abstract groups but clearly not equivalent as permutation groups since the sets (of vertices) on which they act are not equal. (See also Exercise 1.7.)

Note in particular that, if $(\Gamma_1, Y_1) \equiv (\Gamma_2, Y_2)$, then apart from $\Gamma_1 \simeq \Gamma_2$ as abstract groups, and $|Y_1| = |Y_2|$, the cycle structure of the permutations of Γ_1 on Y_1 must be the same as those of Γ_2 on Y_2. However, the converse is not true; that is, Γ_1 and Γ_2 could be isomorphic and the cycle structures of their respective actions could be the same, but (Γ_1, Y_1) might not be equivalent to (Γ_2, Y_2) (see Exercise 1.9).

If (Γ, Y) is a permutation group acting on Y and Y' is a union of orbits of Y, then we can talk about the action of Γ *restricted* to Y', that is, the permutation group (Γ, Y') where, for $\alpha \in \Gamma$ and $y' \in Y'$, $\alpha(y')$ is the same as in (Γ, Y). When Y' is a union of orbits we also say that it is *invariant* under the action of Γ because in this case $\alpha(y') \in Y'$ for all $\alpha \in \Gamma$ and $y' \in Y'$. Also, (Γ', Y') is said to be a subpermutation group of (Γ, Y) if $\Gamma' \leq \Gamma$ and Y' is a union of orbits of Γ' acting on Y.

The following is a useful well-known result on permutation groups whose proof is not difficult and is left as an exercise (see Exercise 1.10).

Theorem 1.1 *Let (Γ, Y) be a permutation group acting transitively on Y. Let $y \in Y$, let $\mathcal{H} = \Gamma_y$ be the stabiliser of y and let W be $\Gamma/\mathcal{H}$, the set of left cosets of $\mathcal{H}$ in Γ. Then (Γ, Y) is equivalent to $(L^{\mathcal{H}}(\Gamma), W)$.*

If (Γ, Y) is not transitive, and $\mathcal{O}$ is the orbit containing y, then $(L^{\mathcal{H}}(\Gamma), W)$ is equivalent to the action of Γ on Y restricted to $\mathcal{O}$.

In the context of groups and graphs we shall need the very important idea of a group acting on pairs of elements of a set. Thus, let (Γ, Y) be a permutation group acting on the set Y. By $(\Gamma, Y \times Y)$ we shall mean the action on ordered pairs of Y induced by Γ as follows: If $\alpha \in \Gamma$ and $x, y \in Y$, then

$$\alpha((x, y)) = (\alpha(x), \alpha(y)).$$

Similarly, by $(\Gamma, \binom{Y}{2})$ we shall mean the action on unordered pairs of distinct elements of Y induced by

$$\alpha(\{x, y\}) = \{\alpha(x), \alpha(y)\}.$$

These ideas will be developed further in a later chapter.

In later chapters we shall also need the notions of k-transitivity and primitivity of a permutation group. In order to study permutation groups in more detail one has to dig deeper into the concept of transitivity. Suppose, for example, that Y is the set $\{1, 2, 3, 4, 5\}$ and Γ is the group generated by the permutation $\alpha = (1\ 2\ 3\ 4\ 5)$. Then clearly the permutation group (Γ, Y) is transitive because for any $i, j \in Y$ there is some power of α which maps i into j. But there is no power of α which, say, simultaneously maps 1 into 5 and 2 into 3. That is, not every ordered pair of distinct elements of Y can be mapped by a permutation in Γ into any other given ordered pair of distinct elements. We therefore say that the permutation group (G, Y) is not 2-transitive.

More generally, a permutation group (Γ, Y) is said to be *k-transitive* if, given any two k-tuples $(x_1, x_2, \ldots, x_k)$ and $(y_1, y_2, \ldots, y_k)$ of distinct elements of Y, then there is an $\alpha \in \Gamma$ such that

$$(\alpha(x_1), \alpha(x_2), \ldots, \alpha(x_k)) = (y_1, y_2, \ldots, y_k).$$

Thus, a transitive permutation group is 1-transitive. Also, (Γ, Y) is said to be *k-homogeneous* if, for any two k-subsets A, B of Y, there is an $\alpha \in \Gamma$ such that $\alpha(A) = B$, where $\alpha(A) = \{\alpha(a) : a \in A\}$.

Finally, let (Γ, Y) be transitive and suppose that $\mathcal{R}$ is an equivalence relation on Y, and let the equivalence classes of Y under $\mathcal{R}$ be $Y_1, Y_2, \ldots, Y_r$. Then (Γ, Y) is said to be *compatible* with $\mathcal{R}$ if, for any $\alpha \in \Gamma$ and any equivalence class Y_i, the set $\alpha(Y_i)$ is also an equivalence class. For example, if $Y = \{1, 2, 3, 4\}$ and Γ is the group generated by the permutation $(1\ 2\ 3\ 4)$, then (Γ, Y) is compatible with the relation whose equivalence classes are $\{1, 3\}$ and $\{2, 4\}$.

Any permutation group is clearly compatible with the trivial equivalence relations on Y, namely, those in which either all of Y is an equivalence class or when each singleton set is an equivalence class. If these are the only equivalence relations with which (Γ, Y) is compatible, then the permutation group is said to be *primitive*. Otherwise it is *imprimitive*.

If (Γ, Y) is imprimitive and $\mathcal{R}$ is a nontrivial equivalence relation on Y with which the permutation group is compatible, then the equivalence classes of $\mathcal{R}$ are called *imprimitivity blocks* and their set Y/R is an *imprimitivity block system* for the permutation group (Γ, Y).

It is an easy exercise (see Exercise 1.14) to show that a 2-transitive permutation group is primitive.

We shall also need some elementary ideas on the presentation of a group in terms of generators and relations.

Let Γ be a group and let $X \subseteq \Gamma$. A *word* in X is a product of a finite number of terms, each of which is an element of X or an inverse of an element of X. The set X is said to *generate* Γ if every element in Γ can be written as a word in X; in this case the elements of X are said to be *generators* of Γ. A *relation* in X is an equality between two words in X. By taking inverses, any relation can be written in the form $w = 1$, where w is some word in X.

If X generates Γ and every relation in Γ can be deduced from one of the relations $w_1 = 1, w_2 = 1, \ldots$ in X, then we write

$$\Gamma = \langle X | w_1 = 1, w_2 = 1, \ldots \rangle.$$

This is called a *presentation* of Γ in terms of generators and relations. The group Γ is said to be *finitely generated* (respectively, *finitely related*) if $|X|$ (respectively, the number of relations) is finite; it is called *finitely presented*, or we say that it has a *finite presentation*, if it is both finitely generated and finitely related.

It is clear that every finite group has a finite presentation (although the converse is false). Simply take $X = \Gamma$ and, as relations, take all expressions of the form $\alpha_i \alpha_j = \alpha_k$ for all $\alpha_i, \alpha_j \in \Gamma$. In other words, the multiplication table of Γ serves as the defining relations.

It is well to point out that removing relations from a presentation of a group in general gives a larger group, the extreme case being that of the *free group* which has only generators and no relations.

The simplest free group is the infinite cyclic group that has the presentation

$$\langle \alpha \rangle$$

with just one generator and no defining relation, whereas the cyclic group of order n has the presentation

$$\langle \alpha | \alpha^n = 1 \rangle;$$

this group is denoted by $\mathbb{Z}_n$.

The group with presentation

$$\langle \alpha, \beta \rangle$$

is the infinite free group on two elements. The dihedral group of degree n is denoted by D_n. It has order $2n$ and also has a presentation with two generators:

$$\langle \alpha, \beta | \alpha^2 = 1, \beta^n = 1, \alpha^{-1}\beta\alpha = \beta^{-1} \rangle.$$

Determining a group from a given presentation is not an easy problem. The reader who doubts this can try to show that the presentations

$$\langle \alpha, \beta : \alpha\beta^2 = \beta^3\alpha, \beta\alpha^2 = \alpha^3\beta \rangle$$

and

$$\langle \alpha, \beta, \gamma : \alpha^3 = \beta^3 = \gamma^3 = 1, \alpha\gamma = \gamma\alpha^{-1}, \alpha\beta\alpha^{-1} = \beta\gamma\beta^{-1} \rangle$$

both give the trivial group. We shall of course make a very simple use of standard group presentations where these difficulties do not arise. The book [159] is a standard reference for advanced work on group presentations.

The reader is referred to [147, 222] for any terms and concepts on group theory that are used but not defined in these chapters and, in particular, to [49, 62] for more information on permutation groups.

1.3 Graphs and groups

Let G, G' be two graphs. A bijection $\alpha : V(G) \to V(G')$ is called an *isomorphism* if

$$\{u, v\} \in E(G) \Leftrightarrow \{\alpha(u), \alpha(v)\} \in E(G').$$

The graphs G, G' are, in this case, said to be *isomorphic*, and this is denoted by $G \simeq G'$. Similarly, if D, D' are digraphs, then a bijection $\alpha : V(D) \to V(D')$ is called an *isomorphism* if

$$(u, v) \in A(D) \Leftrightarrow (\alpha(u), \alpha(v)) \in A(D'),$$

and in this case the digraphs D, D' are also said to be *isomorphic*, and again this is denoted by $D \simeq D'$.

If the two graphs, or digraphs, in this definition are the same, then α is said to be an *automorphism* of G or of D. The set of automorphisms of a graph or a digraph is a group under composition of functions, and it is denoted by Aut(G) or Aut(D).

Note that an automorphism α of G is an element of $S_{V(G)}$, although it is its induced action on $E(G)$ that determines whether α is an automorphism. This fact, although clear from the definition of automorphism, is worth emphasising when beginning to study automorphisms of graphs.

Figure 1.2. No automorphism permutes the edges as (12 23 34)

For example, for the graph in Figure 1.2, the permutation of edges given by (12 23 34) is not induced by any permutation of the vertex-set $\{1, 2, 3, 4\}$. The only automorphisms for this graph are the identity and the permutation $(14)(23)$, which induces the permutation (12 34)(23) of the edges in the graph.

The question of edge permutations not induced by vertex permutations will be considered in some more detail later in this chapter.

The process of obtaining a permutation group from a digraph can be reversed in a very natural manner. Suppose that (Γ, Y) is a group of permutations acting on a set Y. Let A be a union of orbits of $(\Gamma, Y \times Y)$. Clearly, the digraph D whose vertex-set is Y and whose arc-set is A has Γ as a subgroup of its automorphism group. It might, however, happen that $\mathrm{Aut}(G)$ is larger than Γ. Moreover, if the pairs in A are such that, for every $(u, v) \in A$, (v, u) is also in A, then replacing every opposite pair of arcs of D by a single edge gives a graph G such that $\Gamma \subseteq \mathrm{Aut}(G)$.

This and other ways of constructing graphs or digraphs admitting a given group of permutations will be studied in more detail in Chapter 4.

Certain facts about automorphisms of graphs and digraphs are very easy to prove and are therefore left as exercises:

(i) $\mathrm{Aut}(G) = \mathrm{Aut}(\overline{G})$;
(ii) $\mathrm{Aut}(G) = S_{V(G)}$ if and only if G or $\overline{G}$ is K_n, the complete graph on n vertices;
(iii) $\mathrm{Aut}(C_n) = D_n$.

Also, let α be an automorphism of G and u, v vertices of G. Then,

(iv) $\deg(u) = \deg(\alpha(u))$;
(v) $G - u \simeq G - \alpha(u)$;
(vi) $d(u, v) = d(\alpha(u), \alpha(v))$, where $d(u, v)$ is the distance between u and v.

Also, if u is a vertex in a digraph D and α is an automorphism of D, then

(vii) $\deg_{\mathrm{in}}(u) = \deg_{\mathrm{in}}(\alpha(u))$ and $\deg_{\mathrm{out}}(u) = \deg_{\mathrm{out}}(\alpha(u))$.

If u and v are vertices in a graph G and there is an automorphism α of G such that $\alpha(u) = v$, then u and v are said to be *similar*. If $G - u \simeq G - v$, then u and v are said to be *removal-similar*. Property (v) tells us that if two vertices are similar, then they are removal-similar. The converse of this is, however, false, as can be seen from the graph shown in Figure 1.3. Here, the vertices u, v are removal-similar but not similar. Such vertices are called *pseudosimilar*. Similar, removal-similar and pseudosimilar edges are analogously defined: Two edges ab, cd of G are similar if there is an automorphism α of G such that $\alpha(a)\alpha(b) = cd$. We shall be studying pseudosimilarity in more detail in Chapter 5.

Sometimes we ask questions of this type: how many graphs (possibly of some fixed order n) are there? The answer to this question depends heavily on how we consider two graphs to be different.

In general, if the order of a graph G is n, we can think of its vertices as being labelled with the integers $\{1, 2, \ldots, n\}$. Two graphs G and H of order n so labelled are called *identical* or *equal as labelled graphs* (written $G = H$) if

$$ij \in E(G) \Leftrightarrow ij \in E(H).$$

(Compare this definition with that of isomorphic graphs.) Obviously, identical graphs are isomorphic, but the converse is not true. For example, the graphs in Figure 1.4 are isomorphic but not identical.

Counting nonisomorphic graphs is, in general, much more difficult than counting nonidentical graphs. For example, there are four nonisomorphic graphs on three vertices but eight nonidentical ones. These are shown in Figures 1.5 and 1.6, respectively.

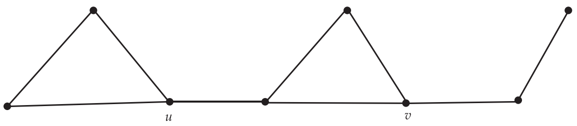

Figure 1.3. A pair of pseudosimilar vertices

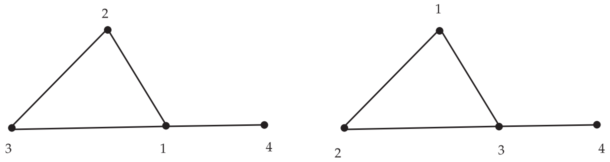

Figure 1.4. Isomorphic but nonidentical graphs

Figure 1.5. The four nonisomorphic graphs of order 3

Cambridge University Press
978-1-316-61044-2 - Topics in Graph Automorphisms and Reconstruction
Josef Lauri and Raffaele Scapellato
Excerpt
More information

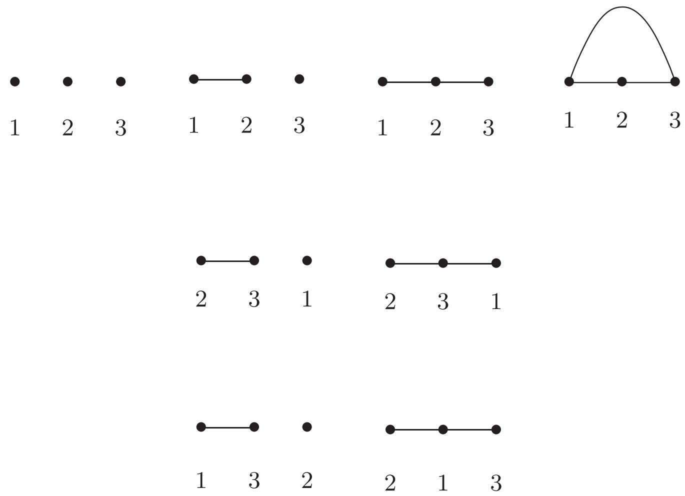

Figure 1.6. The eight nonidentical graphs of order 3

Counting nonisomorphic graphs involves consideration of group symmetries. For more on this the reader is referred to [103].

1.4 Edge-automorphisms and line-graphs

Although we shall be dealing mostly with $\mathrm{Aut}(G)$ and its realisation as the permutation group $(\mathrm{Aut}(G), V(G))$, let us briefly look at other related groups associated with G. In this section we shall assume that G is a nontrivial graph, that is, its edge-set is nonempty.

An *edge-automorphism* of a graph G is a bijection θ on $E(G)$ such that two edges e, f are adjacent in G if and only if $\theta(e), \theta(f)$ are also adjacent in G. The set of all edge-automorphisms of G is a group under composition of functions, and it is denoted by $\mathrm{Aut}_1(G)$.

The concept of edge-automorphisms can perhaps be best understood within the context of line-graphs. The *line-graph* $L(G)$ of a graph G is defined as the graph whose vertex-set is $E(G)$ and in which two vertices are adjacent if and only if the corresponding edges are adjacent in G. An automorphism of $L(G)$ is clearly an edge-automorphism of G and $(\mathrm{Aut}_1(G), E(G))$ is equivalent to $(\mathrm{Aut}(L(G), V(L(G)))$. In this section we shall give the exact relationship between $\mathrm{Aut}_1(G)$ and $\mathrm{Aut}(G)$, that is, between the automorphism groups of G and $L(G)$.

As we described earlier, any automorphism α of G naturally induces a bijection $\hat{\alpha}$ on $E(G)$ defined by $\hat{\alpha}(uv) = \alpha(u)\alpha(v)$. It is an important (and easy to