Author:
Bob Howlett

Group representation theory

Introduction

This course is a mix of group theory and linear algebra, with probably more of the latter than the former. You may need to revise your 2nd year vector space notes!

In mathematics the word "representation" basically means "structure-preserving function". Thus—in group theory and ring theory at least—a representation is a homomorphism. But, more specifically, it should be a homomorphism from an object (group or ring) that one is trying to study to another that is in some way more concrete and hence, one hopes, easier to understand. The two simplest concrete kinds of groups are, firstly, the group of all permutations of an arbitrary set, and, secondly, the group of all invertible linear transformations on an arbitrary vector space. So for groups the most commonly studied representations are permutation representations and linear representations.

Definition. (i) A *permutation representation* of a group G on a set S is a homomorphism from G to the group of all permutations of S.

(ii) A *linear representation* of a group G on a vector space V is a homomorphism from G to the group of all invertible linear transformations of V.

Unless qualified by some other adjective, "representation" usually means "linear representation", and so it is that this course will be concerned with linear representations of groups. We will generally restrict our attention to finite groups and vector spaces over the complex field, as this simplifies things and provides a more complete theory. Although it would be possible to launch immediately into the development of this theory, we will first spend a little time familiarizing ourselves with some small finite groups, so that we will be able subsequently to see how the theory applies in particular examples.

The founder of the subject was Ferdinand Georg Frobenius (1849–1917), who discovered the amazing basic properties of irreducible group characters, publishing them in a series of papers in the 1890's. His student, Issai Schur, was another who made many significant early contributions to the subject. In its modern form the subject owes much to the contributions of Emmy Noether (in the 1920's), whose work forms the basis of what is now called " modern algebra". Building on this, Richard Brauer developed modular representation theory, in which representations over fields of nonzero characteristic are studied and related to complex representations.

Groups, and examples of groups

Groups were invented as a tool for studying symmetrical objects. These can be objects of any kind at all. If we define a *symmetry* of an object to be a transformation of that object which preserves its essential structure, then the set of all symmetries of the object forms a group. In mathematics it is always possible to regard any object as a set with some additional structure; thus a symmetry is a structure-preserving bijective function from the set to itself. Composition of functions provides an operation on this set, and it is not hard to show that the group axioms must be satisfied.

For example, a field is a set equipped with operations of addition and multiplication, satisfying various axioms. A square can be regarded as a set of points and lines in the Euclidean plane that satisfy various properties to do with angles and distances. A symmetry of a field is a bijective function from the field to itself which preserves the addition and multiplication operations. (That is, a symmetry of a field is an automorphism of the field.) A symmetry of a square is a function from the relevant set of points and lines to itself which preserves all the angles and distances. In both these cases the set of all symmetries is a group.

It is clear that the composite of two functions which both preserve some property will also preserve that property. For example, if R is a set equipped with an operation $*$ (such as addition or multiplication) and if f, $g\colon R \to R$ are functions that both preserve $*$, then for all x, $y \in R$

$$(fg)(x * y) = f(g(x * y)) = f((gx) * (gy)) = (f(gx)) * (f(gy)) = ((fg)x) * ((fg)y),$$

so that fg also preserves $*$. Similarly, if S is a set of points in the Euclidean plane and ϕ, $\psi\colon S \to S$ are functions which preserve angles, then for all P_1, P_2, $P_3 \in S$,

$$\begin{aligned} \angle P_1P_2P_3 &= \angle P_1'P_2'P_3', &&\text{where } P_i' = \psi P_i \\ &= \angle P_1''P_2''P_3'', &&\text{where } P_i'' = \phi P_i' = (\phi\psi)P_i, \end{aligned}$$

so that $\phi\psi$ also preserves angles. Thus it can be seen that the composite of two symmetries if a symmetry. Similarly, the inverse of a symmetry is also a symmetry. Furthermore, composition of functions is an associative operation. So the group axioms are satisfied. We can hope that understanding the symmetry group of an object can lead to a deeper understanding of the object itself.

Representation theory actually reverses this philosophy. If one regards groups as things which are of interest in their own right, then perhaps one can hope to better understand a given group by discovering an object of which the group is the symmetry group, and using properties of that object to uncover information about the group. However, the underlying theme is still that the elements of a group should be associated with transformations of a set. Hence the following definition is natural.

Definition. An action of a group G on a set S is a function $(g, s) \mapsto gs$ from $G \times S$ to S such that
(i) $(gh)s = g(hs)$ for all g, $h \in G$ and $s \in S$,
(ii) $1s = s$ for all $s \in S$, where 1 is the identity element of G.

Note that we will usually use the notation "1" for the identity element of an abstract group, although if the group operation is written as "+" then we will use "0" for the identity. For a group of transformations of a set the identity element will be the identity function from the set to itself, and this we will denote by "id". The identity matrix will be denoted by "I".

Observe that an action of G on S can be viewed as a rule for multiplying elements of S by elements of G, so that the result is another element of S.

We turn now to a discussion of some examples of groups. The cyclic group C_n consists of the n elements 1, x, x^2, $\ldots$, x^{n-1}, where $x^n = 1$. This group can be represented as the group of all rotations of the plane which carry a regular n-sided polygon to itself, x being represented as a rotation through $2\pi/n$. Alternatively one can think of the additive group of $\mathbb{Z}_n$, the ring of integers modulo n, identifying the generator x of C_n with $1 \in \mathbb{Z}_n$, and the identity element of C_n with $0 \in \mathbb{Z}_n$. Another realization of this group is obtained by identifying x^k with the complex number $e^{k(2\pi i/n)}$, with the group operation being the usual multiplication of complex numbers. We can obtain a permutation representation of C_n on the set $\{1, 2, \ldots, n\}$ by mapping x to the permutation σ defined by $\sigma i = i + 1$ for $1 \le i \le n - 1$ and $\sigma n = 1$, and we can obtain a matrix representation of C_n by mapping x to the 2×2 matrix $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, where $\theta = 2\pi/n$.

At this point the student would be right to complain that no proper definition of C_n has been given. What *is* this cyclic group, really? Are its elements the symbols x^k, and if we had written

y^k instead would it be the same group or a different one? Or are the elements of C_n really integers modulo n, or complex nth roots of 1, or perhaps certain permutations or certain matrices? In fact, to talk of *the* cyclic group of order n, as group theorists do, is to be rather imprecise. The five examples we gave above can all be called cyclic groups of order n. The crucial fact, though, is that any two cyclic groups of order n are isomorphic to each other: if G and H are both cyclic groups of order n then there is a one to one correspondence between the elements of G and the elements of H which respects the two group operations. When a group theorist says "there is only one cyclic group of order n", what is meant is that there is only one isomorphism class of cyclic groups of order n. If one really wanted to have a single object called the cyclic group of order n, it would have to be in fact an isomorphism class of groups, rather than a group!

Before proceeding farther with examples of groups we need a notation for permutations. A permutation of a set is a bijective function from the set to itself. If σ is a permutation of $\{1, 2, \ldots, n\}$ then $\sigma 1$, $\sigma 2$, …, σn are 1, 2, …, n in some order, and we write $\sigma = \begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma 1 & \sigma 2 & \cdots & \sigma n \end{bmatrix}$. Thus, for example, $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{bmatrix}$ denotes the function $\sigma\colon \{1,2,3,4,5\} \to \{1,2,3,4,5\}$ such that $\sigma 1 = 4$, $\sigma 2 = 1$, $\sigma 3 = 5$, $\sigma 4 = 2$ and $\sigma 5 = 3$. Having introduced this notation I want to immediately abandon it in favour of the more compact "cycle notation", which renders the above permutation as $(1,4,2)(3,5)$. In the cycle notation for σ the elements of the set $\{1, 2, \ldots, n\}$ are gathered into sequences in which each successive term is obtained by applying σ to the one before it, and σ applied to the last term of a sequence gives the first. Sequences with just one term k correspond to those k for which $\sigma k = k$, and these are often omitted. Thus in the cycle notation the permutation $\tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{bmatrix}$ is usually written as $(1,3,4)$, but is sometimes written as $(1,3,4)(2)(5)$, especially if it is not otherwise clear from the context that τ is a permutation of $\{1,2,3,4,5\}$ rather than $\{1,2,3,4\}$.

The composite of two permutations σ and τ of the same set is the function $\sigma\tau$ defined by $(\sigma\tau)k = \sigma(\tau k)$ for each k. As the composite of two bijections is a bijection it follows that $\sigma\tau$ is a permutation. The set of all permutations of a given set S forms a group, called the symmetric group on S, and sometimes denoted by $\mathrm{Sym}(S)$. If the number of elements in S is n then $\mathrm{Sym}(S)$ is called the symmetric group of degree n, commonly written as S_n. Of course there is really a symmetric group of degree n for every n-element set, but they are all isomorphic to one another, and in any case it is natural and customary to use the set $\{1, 2, \ldots, n\}$ as the standard n-element set (unless the context favours some other choice). Observe that the group S_3 has six elements, namely id, $(1,2)$, $(1,3)$, $(2,3)$, $(1,2,3)$ and $(1,3,2)$. The multiplication table for this group is as follows.

S_3	id	(123)	(132)	(12)	(13)	(23)
id	id	(123)	(132)	(12)	(13)	(23)
(123)	(123)	(132)	id	(13)	(23)	(12)
(132)	(132)	id	(123)	(23)	(12)	(13)
(12)	(12)	(23)	(13)	id	(132)	(123)
(13)	(13)	(12)	(23)	(123)	id	(132)
(23)	(23)	(13)	(12)	(132)	(123)	id

Let us check one entry in this table. If $\sigma = (1,2,3)$ and $\tau = (1,3)$ then

$$(\sigma\tau)1 = \sigma(\tau 1) = \sigma 3 = 1,$$

$$(\sigma\tau)2 = \sigma(\tau 2) = \sigma 2 = 3,$$
$$(\sigma\tau)3 = \sigma(\tau 3) = \sigma 1 = 2,$$

so that $\sigma\tau = (2, 3)$, in agreement with the table.

Maintaining the notation $\sigma = (1, 2, 3)$ and $\tau = (1, 3)$, observe that $\tau\sigma\tau = (1, 3, 2) = \sigma^{-1}$. This relation enables one to rewrite any product of powers of σ and powers of τ so that the powers of σ precede the powers of τ. Since $\tau = \tau^{-1}$ the relation $\tau\sigma\tau = \sigma^{-1}$ can alternatively be written as $\tau\sigma = \sigma^{-1}\tau$ or as $\tau\sigma^{-1} = \sigma\tau$; in consequence one can always move τ past σ^{ϵ} at the expense of replacing σ^{ϵ} by $\sigma^{-\epsilon}$. For example,

$$(\sigma^2\tau)(\sigma\tau) = \sigma^2(\sigma^{-1}\tau)\tau = \sigma.$$

Such considerations, when combined with the fact that $\sigma^3 = \mathrm{id}$, make it clear that the product of any two elements of the set $\{\mathrm{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ will always be another element of the same set. Furthermore, if $\sigma^i\tau^j = \sigma^k\tau^l$ then $\sigma^{i-k} = \tau^{l-j}$; however, the only permutation which is both a power of σ and a power of τ is id, and so it follows that $\sigma^i = \sigma^k$ and $\tau^j = \tau^l$. The six expressions $\sigma^i\tau^j$ for $i \in \{0, 1, 2\}$ and $j \in \{0, 1\}$ thus correspond to six distinct elements of the group, and as S_3 has only six elements altogether, we have them all. The upshot of this is that the structure of S_3 is completely determined by the relations $\sigma^3 = \tau^2 = \mathrm{id}$ and $\tau\sigma\tau = \sigma^{-1}$.

Observe that S_3 is isomorphic to the group of all symmetries of an equilateral triangle. Labelling the vertices of the triangle as 1, 2 and 3 permits us to identify the symmetries with permutations of the vertices, and we see that there are three rotation symmetries (through angles of 0, $2\pi/3$ and $4\pi/3$) corresponding to the permutations id, $(1, 2, 3)$ and $(1, 3, 2)$, and three reflection symmetries corresponding to the other three elements of S_3. (For example, the reflection in the perpendicular bisector of the side joining vertex 1 and vertex 2 interchanges these two vertices and fixes the other, and thus corresponds to the permutation $(1, 2)$.)

The group of all symmetries of a regular n-sided polygon is known as the *dihedral group* of order $2n$. Many authors denote this group by D_{2n}, and many others denote it by D_n. There are n rotation symmetries, through angles of $2k\pi/n$, where $k \in \{1, 2, \ldots, n-1\}$, and there are n reflection symmetries, in the n lines which are the bisectors of the internal angles and the perpendicular bisectors of the sides. (Note that if n is even then for each side of the polygon there is an opposite side, and the perpendicular bisectors of these two sides are the same. Likewise, the bisector of the angle at a vertex coincides with the bisector of the angle at the opposite vertex. If n is odd then the bisector of an angle coincides with the perpendicular bisector of the opposite side.) If we let σ be the clockwise rotation through $2\pi/n$ and let τ be any of the reflections then it is fairly easy to check that the following relations are satisfied: $\sigma^n = \tau^2 = \mathrm{id}$, and $\tau\sigma\tau = \sigma^{-1}$. As in the case $n = 3$, dealt with above, we see that the $2n$ elements of the group are id, σ, σ^2, …, σ^{n-1}, τ, $\sigma\tau$, $\sigma^2\tau$, …, $\sigma^{n-1}\tau$. Furthermore, the multiplication table is completely determined by the relations we have written down. It is also straightforward to represent the dihedral group as a group of permutations. Numbering the vertices of the regular polygon 1, 2, …, n (clockwise), the rotation σ corresponds to the n-cycle $(1, 2, \ldots, n)$, while the reflection in the perpendicular bisector of the side joining vertices 1 and n corresponds to the permutation $(1, n)(2, n-1)(3, n-2)\cdots$, where the last factor is $(k, k+1)$ if $n = 2k$ is even, or $(k-1, k+1)$ if $n = 2k-1$ is odd.

We can obtain an interesting group with 21 elements, which are permutations of the set $\{1, 2, 3, 4, 5, 6, 7\}$, in the following manner. Let $a = (1, 2, 3, 4, 5, 6, 7)$ and let $b = (2, 3, 5)(4, 7, 6)$. Clearly $a^7 = \mathrm{id}$ and $b^3 = \mathrm{id}$. (For example, $b^3 2 = b(b(b2)) = b(b3) = b5 = 2$.) It is also easy to check that

$$\begin{aligned} bab^{-1} &= (2, 3, 5)(4, 7, 6)(1, 2, 3, 4, 5, 6, 7)(7, 6, 4)(5, 3, 2) \\ &= (1, 3, 5, 7, 2, 4, 6) \\ &= a^2. \end{aligned}$$

So $ba = a^2b$, and this relation enables us to rewrite any product of powers of a and powers of b so that all the powers of a precede all the powers of b. For example,

$$\begin{aligned}(ab^2)(a^2b) &= ab(ba)ab = ab(a^2b)ab = aba^2(ba)b = aba^2(a^2b)b = a(ba)a^3b^2 \\ &= a(a^2b)a^3b^2 = a^3(ba)a^2b^2 = a^3(a^2b)a^2b^2 = a^5(ba)ab^2 = a^5(a^2b)ab^2 = (ba)b^2 = a^2b^3.\end{aligned}$$

It follows that the product of any two elements of the set $\{\, a^ib^j \mid 0 \le i6,\ 0 \le j \le 2 \,\}$ is also in this set. The non-identity powers of a are all 7-cycles, and since no power of b is a 7-cycle it follows that the only element which is simultaneously a power of a and a power of b is the identity. Now if $a^ib^j = a^kb^l$ then $a^{i-k} = b^{l-j}$, which must be the identity, whence $a^i = a^k$ and $b^j = b^l$. So there are 21 distinct elements in the above set, and it is not hard to see that they must constitute a group.

This group—or, rather, a group isomorphic to this group—can also be constructed by use of matrices. Let $\omega = e^{2\pi i/7}$, and let

$$a = \begin{pmatrix} \omega & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & \omega^4 \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

It is a straightforward matter to check that the relations $a^7 = b^3 = I$ and $bab^{-1} = a^2$ are satisfied.

Lecture 2, 30/7/97

Group actions

We have defined the concepts of an action of a group G on a set S and of a permutation representation of G on S. In fact these two concepts are essentially equivalent. Suppose that $\phi: G \to \mathrm{Sym}(S)$ is a permutation representation of G. Then ϕg is a permutation of S whenever $g \in G$, and so for each $x \in S$ we can define $gx \in S$ by the formula $gx = (\phi g)x$. Since ϕ is a homomorphism we have that $\phi(gh) = (\phi g)(\phi h)$ for all $g, h \in G$, and since the product of the permutations ϕg and ϕh is by definition their composite (ϕh followed by ϕg), it follows that

$$(gh)x = (\phi(gh))x = ((\phi g)(\phi h))x = (\phi g)((\phi h)x) = (\phi g)(hx) = g(hx)$$

for all $x \in S$. This shows that the first property in the definition of a group action is satisfied. Furthermore, since a group homomorphism necessarily takes the identity element to the identity element, we must have that $\phi 1 = \mathrm{id}$, and hence

$$1x = (\phi 1)x = id(x) = x$$

for all $x \in S$. Thus the second requirement is also satisfied, and we have an action of G on S. Conversely, if we are given an action of G on S then for each $g \in G$ we can define a function $\phi g: S \to S$ by $(\phi g)x = gx$. Then for all $g, h \in G$ and $x \in S$ we have that

$$((\phi g)(\phi h))x = (\phi g)((\phi h)x) = (\phi g)(hx) = g(hx) = (gh)x = (\phi(gh))x,$$

and thus $(\phi g)(\phi h) = \phi(gh)$. Furthermore, $\phi 1 = \mathrm{id}$, since

$$(\phi 1)x = 1x = x = \mathrm{id}(x)$$

for all $x \in S$. It follows that $(\phi g)(\phi(g^{-1})) = \mathrm{id} = (\phi(g^{-1}))(\phi g)$, and so the functions ϕg and $\phi(g^{-1})$ are inverse to each other, which means that they are both bijective. So ϕ is a function from G

to $\mathrm{Sym}(S)$, and as we have already shown that it preserves multiplication, it follows that ϕ is a permutation representation.

It is a rather common practice amongst algebraists, especially group theorists, for functions to be written as right operators rather than left operators. In other words, the value of the function f at the element x is written as xf rather than $f(x)$. Although this is purely a notational matter, it has ramifications. In particular, the composite fg of two functions f and g is defined by the rule $x(fg) = (xf)g$ if f and g are written as right operators, whereas for left operators the corresponding formula for fg is $(fg)(x) = f(g(x))$. Under the right operator convention, fg means f followed by g; under the left operator convention it means g followed by f. As there are contexts in which both right operators and left operators appear simultaneously, we have to be able to work with both conventions. Accordingly, we define a *right action* of a group G on a set S to be a function $(x, g) \mapsto xg$ from $S \times G$ to S such that $x1 = x$ and $x(gh) = (xg)h$ for all g, $h \in G$ and all $x \in S$. If onen were to write one's permutations as right operators rather than left operators—and in fact for permutations the right operator convention is more common than the left operator convention—then a permutation representation of G on S would be essentially the same as a right action of G on S.

If the set S on which a group acts happens not to be just a set, but a set with some additional structure, then it is natural ask whether the action preserves the structure. Thus, for example, a left action of a group G on a vector space V implicitly means a left action of G on the set V such that $g(u + v) = gu + gv$ and $g(\lambda v) = \lambda(gv)$ for all u, $v \in V$ and all scalars λ and all $g \in G$. A left action of G on V is then essentially the same as a homomorphism from G to the group of all invertible linear transformations on V (where the linear transformations are written as left operators).

We can also talk of an action of a group on another group. It is common to use a right operator convention, and to write the operators as exponents. Following this convention, an action of a group A on another group G is a function $(g, \alpha) \mapsto g^\alpha$ from $G \times A$ to G such that the following properties are satisfied:

(i) $(g^\alpha)^\beta = g^{\alpha\beta}$ for all $g \in G$ and α, $\beta \in A$,

(ii) $g^1 = g$ for all $g \in G$ (where 1 is the identity element of A),

(iii) $(gh)^\alpha = g^\alpha h^\alpha$ for all g, $h \in G$ and $\alpha \in A$.

Recall that a normal subgroup K of a group G is a subgroup of G such that $g^{-1}kg \in K$ for all $g \in G$ and $k \in K$. It is an important basic theorem of group theory that if K is normal in G then there is an action of G on K defined by $k^g = g^{-1}kg$ for all $g \in G$ and $k \in K$. It is a straightforward matter to check that the three properties above are satisfied. For example, if k_1, $k_2 \in K$ and $g \in G$ then

$$(k_1k_2)^g = g^{-1}k_1k_2g = (g^{-1}k_1g)(g^{-1}k_2g) = k_1^g k_2^g.$$

If G and H are groups the *external direct product* of G and H is the set

$$G \times H = \{\, (g, h) \mid g \in G,\ h \in H \,\},$$

equipped with multiplication defined by $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$. It is readily checked that $G \times H$ is a group under this operation.

Suppose that S and T are subgroups of G such that $S \cap T = \{1\}$, and suppose also that $st = ts$ for all $s \in S$ and $t \in T$. Define a function f from the external direct product $S \times T$ to G by $f(s, t) = st$ for all $s \in S$ and $t \in T$. Clearly f is a homomorphism:

$$f((s_1, t_1)(s_2, t_2)) = f(s_1s_2, t_1t_2) = (s_1s_2)(t_1t_2) = (s_1t_1)(s_2t_2) = f(s_1, t_1)f(s_2, t_2).$$

It is also easy to show that f is injective: if $f(s, t) = 1$ then $st = 1$, and so $s = t^{-1} \in S \cap T = \{1\}$, whence $(s, t) = (1, 1)$, which is the identity element of $S \times T$. So the kernel of f is trivial, whence f

is injective, as claimed. If it is also the case that $G = ST$, so that every element of G is expressible in the form st with $s \in S$ and $t \in T$, then is follows that f is an isomorphism from $S \times T$ to G.

Definition. A group G is said to be the *internal direct product* of S and T if S and T are subgroups of G such that $S \cap T = \{1\}$ and $ST = G$, and $st = ts$ for all $s \in S$ and $t \in T$.

If S, T are subgroups of G such that $S \cap T = \{1\}$ and $G = ST$ then the the extra condition that $st = ts$ for all $s \in S$ and $t \in T$ is equivalent to the condition that S and T are both normal subgroups. For suppose that S and T are both normal, and let $s \in S$ and $t \in T$. Normality of T implies that $s^{-1}ts \in T$, and so $t^{-1}s^{-1}ts \in T$. On the other hand, normality of S implies that $t^{-1}s^{-1}t \in S$, whence $t^{-1}s^{-1}ts \in S$. So $t^{-1}s^{-1}ts \in S \cap T = \{1\}$, so that $t^{-1}s^{-1}ts = 1$, and $ts = st$. Conversely, if we assume that elements of S and T commute then for $s \in S$ and $t, t' \in T$ we have that $(st)^{-1}t'(st)^{-1} = t^{-1}s^{-1}t'st = t^{-1}t't \in T$. But as $G = ST$ every element of G is expressible in the form st, and it follows that $g^{-1}tg \in T$ for all $g \in G$ and $t' \in T$; that is, T is normal. Similarly, S is also normal.

If a group S has an action on another group T then we can define a *semidirect product* $S \ltimes T$ of S and T as follows. The elements of $S \ltimes T$ are ordered pairs (s, t) (where $s \in S$ and $t \in T$). Multiplication of ordered pairs is defined by the rule

$$(s_1, t_1)(s_2, t_2) = (s_1 s_2, t_1^{s_2} t_2).$$

It is left as an exercise for the student to prove that the group axioms are satisfied.

A group G is an internal semidirect product of its subgroups S and T if $G = ST$ and $S \cap T = \{1\}$, and the subgroup T is normal. Under these circumstances S has an action on T given by $t^s = s^{-1}ts$ for all $s \in S$ and $t \in T$, and it is now routine to check that $(s, t) \mapsto st$ provides an isomorphism from $S \ltimes T$ to G.