Semidirect products

GU4041

Columbia University

November 28, 2023

Outline

Automorphisms of normal subgroups

Let $N \trianglelefteq G$ be a normal subgroup. For any $g \in G$, the conjugation map on N

$$n \mapsto r_g(n) := gng^{-1}, \;\; n \in N$$

is an automorphism of N.

This is because if $n_1, n_2 \in N$

$$r_g(n_1 \cdot n_2) = gn_1 \cdot n_2 g^{-1} = gn_1 g^{-1} \cdot gn_2 g^{-1} = r_g(n_1) \cdot r_g(n_2).$$

The set $Aut(N)$ of automorphisms of N is a *group* under composition.

Lemma

The map $g \mapsto r_g$ is a homomorphism of groups:

$$G \to Aut(N).$$

Automorphisms of normal subgroups

Let $N \trianglelefteq G$ be a normal subgroup. For any $g \in G$, the conjugation map on N

$$n \mapsto r_g(n) := gng^{-1}, \ \ n \in N$$

is an automorphism of N.
This is because if $n_1, n_2 \in N$

$$r_g(n_1 \cdot n_2) = gn_1 \cdot n_2g^{-1} = gn_1g^{-1} \cdot gn_2g^{-1} = r_g(n_1) \cdot r_g(n_2).$$

The set $Aut(N)$ of automorphisms of N is a *group* under composition.

Lemma

The map $g \mapsto r_g$ is a homomorphism of groups:

$$G \to Aut(N).$$

Automorphisms of normal subgroups

Let $N \trianglelefteq G$ be a normal subgroup. For any $g \in G$, the conjugation map on N

$$n \mapsto r_g(n) := gng^{-1}, \ \ n \in N$$

is an automorphism of N.
This is because if $n_1, n_2 \in N$

$$r_g(n_1 \cdot n_2) = gn_1 \cdot n_2g^{-1} = gn_1g^{-1} \cdot gn_2g^{-1} = r_g(n_1) \cdot r_g(n_2).$$

The set $Aut(N)$ of automorphisms of N is a *group* under composition.

Lemma

The map $g \mapsto r_g$ is a homomorphism of groups:

$$G \to Aut(N).$$

Automorphisms of normal subgroups

Let $N \trianglelefteq G$ be a normal subgroup. For any $g \in G$, the conjugation map on N

$$n \mapsto r_g(n) := gng^{-1}, \ \ n \in N$$

is an automorphism of N.
This is because if $n_1, n_2 \in N$

$$r_g(n_1 \cdot n_2) = gn_1 \cdot n_2 g^{-1} = gn_1 g^{-1} \cdot gn_2 g^{-1} = r_g(n_1) \cdot r_g(n_2).$$

The set $Aut(N)$ of automorphisms of N is a *group* under composition.

Lemma

The map $g \mapsto r_g$ is a homomorphism of groups:

$$G \to Aut(N).$$

Proof of the lemma

Proof.

We need to show that if $g, h \in G$, then

$$r_{gh} = r_g \circ r_h.$$

That is, for all $n \in N$,

$$r_{gh}(n) = r_g \circ r_h(n) = r_g(r_h(n)).$$

We check:

$$r_g(r_h(n)) = r_g(hnh^{-1}) = g(hnh^{-1})g^{-1} = (gh)n(gh)^{-1} = r_{gh}(n).$$

Proof of the lemma

Proof.

We need to show that if $g, h \in G$, then

$$r_{gh} = r_g \circ r_h.$$

That is, for all $n \in N$,

$$r_{gh}(n) = r_g \circ r_h(n) = r_g(r_h(n)).$$

We check:

$$r_g(r_h(n)) = r_g(hnh^{-1}) = g(hnh^{-1})g^{-1} = (gh)n(gh)^{-1} = r_{gh}(n).$$

□

Proof of the lemma

Proof.

We need to show that if $g, h \in G$, then

$$r_{gh} = r_g \circ r_h.$$

That is, for all $n \in N$,

$$r_{gh}(n) = r_g \circ r_h(n) = r_g(r_h(n)).$$

We check:

$$r_g(r_h(n)) = r_g(hnh^{-1}) = g(hnh^{-1})g^{-1} = (gh)n(gh)^{-1} = r_{gh}(n).$$

□

Groups of order 6

Proposition

The only groups of order 6 *are* $\mathbb{Z}_6$ *and* D_6.

Proof.

Let G be a group of order 6. If G has an element of order 6 then it is cyclic.

So suppose G has no element of order 6. Suppose G has an element r of order 3. Then the subgroup $N = \langle r \rangle \subset G$ is of index 2, hence is normal. Let $r : G \to Aut(N)$ be the conjugation map. If r is trivial then G is abelian, hence isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3 \xrightarrow{\sim} \mathbb{Z}_6$. Suppose r is not trivial. Then G is a non-abelian group of order 6, with a commutative normal subgroup N of order 3. Let $f \in G, f \notin N$. Then $r(f)$ is the non-trivial automorphism $n \mapsto n^{-1}$ of N. One sees that G is isomorphic to D_6.

Groups of order 6

Proposition

The only groups of order 6 *are* $\mathbb{Z}_6$ *and* D_6.

Proof.

Let G be a group of order 6. If G has an element of order 6 then it is cyclic.

So suppose G has no element of order 6. Suppose G has an element r of order 3. Then the subgroup $N = \langle r \rangle \subset G$ is of index 2, hence is normal. Let $r : G \to Aut(N)$ be the conjugation map. If r is trivial then G is abelian, hence isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3 \xrightarrow{\sim} \mathbb{Z}_6$. Suppose r is not trivial. Then G is a non-abelian group of order 6, with a commutative normal subgroup N of order 3. Let $f \in G, f \notin N$. Then $r(f)$ is the non-trivial automorphism $n \mapsto n^{-1}$ of N. One sees that G is isomorphic to D_6.

Groups of order 6

Proposition

The only groups of order 6 *are* $\mathbb{Z}_6$ *and* D_6.

Proof.

Let G be a group of order 6. If G has an element of order 6 then it is cyclic.

So suppose G has no element of order 6. Suppose G has an element r of order 3. Then the subgroup $N = \langle r \rangle \subset G$ is of index 2, hence is normal. Let $r : G \to Aut(N)$ be the conjugation map. If r is trivial then G is abelian, hence isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3 \xrightarrow{\sim} \mathbb{Z}_6$. Suppose r is not trivial. Then G is a non-abelian group of order 6, with a commutative normal subgroup N of order 3. Let $f \in G, f \notin N$. Then $r(f)$ is the non-trivial automorphism $n \mapsto n^{-1}$ of N. One sees that G is isomorphic to D_6.

Groups of order 6

Proposition

The only groups of order 6 *are* $\mathbb{Z}_6$ *and* D_6.

Proof.

Let G be a group of order 6. If G has an element of order 6 then it is cyclic.

So suppose G has no element of order 6. Suppose G has an element r of order 3. Then the subgroup $N = \langle r \rangle \subset G$ is of index 2, hence is normal. Let $r : G \to Aut(N)$ be the conjugation map. If r is trivial then G is abelian, hence isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3 \xrightarrow{\sim} \mathbb{Z}_6$. Suppose r is not trivial. Then G is a non-abelian group of order 6, with a commutative normal subgroup N of order 3. Let $f \in G, f \notin N$. Then $r(f)$ is the non-trivial automorphism $n \mapsto n^{-1}$ of N. One sees that G is isomorphic to D_6.

□

Groups of order 6

Proof.

Finally, if G has no element of order 3, then it has only elements of order 2. By a homework problem, G is abelian, but then by classification it must be $\mathbb{Z}_6$ again. □

Constructing new groups

Now suppose N and H are groups and

$$r : H \to Aut(N)$$

is a homomorphism. We construct a new group $N \rtimes H$ as follows:
The elements of $N \rtimes H$ are ordered pairs $(n, h), n \in N, h \in H$.
Mutliplication is given by

$$(n_1, h_1)(n_2, h_2) = (n_1 \cdot r(h_1)(n_2), h_1 \cdot h_2).$$

We can remove the parentheses if we take care:

$$(n_1 \cdot h_1)(n_2 \cdot h_2) = n_1(h_1 \cdot n_2)h_2$$

and use the *commutation rule*

$$h_1 \cdot n_2 = h_1 n_2 h_1^{-1} h_1 = r(h_1)(n_2) \cdot h_1.$$

so that

$$(n_1 \cdot h_1)(n_2 \cdot h_2) = n_1(h_1 \cdot n_2)h_2 = n_1 r(h_1)(n_2) \cdot h_1 h_2$$

Constructing new groups

Now suppose N and H are groups and

$$r : H \to Aut(N)$$

is a homomorphism. We construct a new group $N \rtimes H$ as follows: The elements of $N \rtimes H$ are ordered pairs $(n, h), n \in N, h \in H$. Mutliplication is given by

$$(n_1, h_1)(n_2, h_2) = (n_1 \cdot r(h_1)(n_2), h_1 \cdot h_2).$$

We can remove the parentheses if we take care:

$$(n_1 \cdot h_1)(n_2 \cdot h_2) = n_1(h_1 \cdot n_2)h_2$$

and use the *commutation rule*

$$h_1 \cdot n_2 = h_1 n_2 h_1^{-1} h_1 = r(h_1)(n_2) \cdot h_1.$$

so that

$$(n_1 \cdot h_1)(n_2 \cdot h_2) = n_1(h_1 \cdot n_2)h_2 = n_1 r(h_1)(n_2) \cdot h_1 h_2$$

Constructing new groups

Now suppose N and H are groups and

$$r : H \to Aut(N)$$

is a homomorphism. We construct a new group $N \rtimes H$ as follows: The elements of $N \rtimes H$ are ordered pairs $(n, h), n \in N, h \in H$. Mutliplication is given by

$$(n_1, h_1)(n_2, h_2) = (n_1 \cdot r(h_1)(n_2), h_1 \cdot h_2).$$

We can remove the parentheses if we take care:

$$(n_1 \cdot h_1)(n_2 \cdot h_2) = n_1(h_1 \cdot n_2)h_2$$

and use the *commutation rule*

$$h_1 \cdot n_2 = h_1 n_2 h_1^{-1} h_1 = r(h_1)(n_2) \cdot h_1.$$

so that

$$(n_1 \cdot h_1)(n_2 \cdot h_2) = n_1(h_1 \cdot n_2)h_2 = n_1 r(h_1)(n_2) \cdot h_1 h_2$$

Constructing new groups

Now suppose N and H are groups and

$$r : H \to Aut(N)$$

is a homomorphism. We construct a new group $N \rtimes H$ as follows: The elements of $N \rtimes H$ are ordered pairs $(n, h), n \in N, h \in H$. Mutliplication is given by

$$(n_1, h_1)(n_2, h_2) = (n_1 \cdot r(h_1)(n_2), h_1 \cdot h_2).$$

We can remove the parentheses if we take care:

$$(n_1 \cdot h_1)(n_2 \cdot h_2) = n_1(h_1 \cdot n_2)h_2$$

and use the *commutation rule*

$$h_1 \cdot n_2 = h_1 n_2 h_1^{-1} h_1 = r(h_1)(n_2) \cdot h_1.$$

so that

$$(n_1 \cdot h_1)(n_2 \cdot h_2) = n_1(h_1 \cdot n_2)h_2 = n_1 r(h_1)(n_2) \cdot h_1 h_2$$

Examples of semidirect products

In other words, inside $N \rtimes H$ the homomorphism $r : H \to Aut(N)$ corresponds to conjugation of N by H.

The group $N \rtimes H$ is called the *semidirect product* of N and H. The roles of N and H cannot be exchanged.

Example

For any cyclic group $\mathbb{Z}_n$, there is a homomorphism $r : \{\pm 1\} \to Aut(\mathbb{Z}_n)$:

$$r(-1)(x) = -x.$$

The semidirect product $\mathbb{Z}_n \rtimes \{\pm 1\}$ is just the dihedral group D_{2n}.

Examples of semidirect products

In other words, inside $N \rtimes H$ the homomorphism $r : H \to Aut(N)$ corresponds to conjugation of N by H.
The group $N \rtimes H$ is called the *semidirect product* of N and H. The roles of N and H cannot be exchanged.

Example

For any cyclic group $\mathbb{Z}_n$, there is a homomorphism $r : \{\pm 1\} \to Aut(\mathbb{Z}_n)$:

$$r(-1)(x) = -x.$$

The semidirect product $\mathbb{Z}_n \rtimes \{\pm 1\}$ is just the dihedral group D_{2n}.

The semidirect product is a group

We need to prove that multiplication in $N \rtimes H$ is associative and that the identity and inverses exist. The identity is obvious: if we set $e = (e_N, e_H)$, then

$$(e_N, e_H)(n, h) = (e_N \cdot r(e_H)(n), e_H \cdot h)) = (e_N \cdot n, e_H \cdot h) = (n, h)$$

because $r(e_H)$ is the identity in $Aut(N)$.
The identity relation of multiplication on the right is verified in the same way.
Finding the inverse involves solving an equation. Given (n, h), we need to find (n', h') such that

$$(n', h')(n, h) = (e_N, e_H).$$

The semidirect product is a group

We need to prove that multiplication in $N \rtimes H$ is associative and that the identity and inverses exist. The identity is obvious: if we set $e = (e_N, e_H)$, then

$$(e_N, e_H)(n, h) = (e_N \cdot r(e_H)(n), e_H \cdot h)) = (e_N \cdot n, e_H \cdot h) = (n, h)$$

because $r(e_H)$ is the identity in $Aut(N)$.

The identity relation of multiplication on the right is verified in the same way.

Finding the inverse involves solving an equation. Given (n, h), we need to find (n', h') such that

$$(n', h')(n, h) = (e_N, e_H).$$

The semidirect product is a group

We need to prove that multiplication in $N \rtimes H$ is associative and that the identity and inverses exist. The identity is obvious: if we set $e = (e_N, e_H)$, then

$$(e_N, e_H)(n, h) = (e_N \cdot r(e_H)(n), e_H \cdot h)) = (e_N \cdot n, e_H \cdot h) = (n, h)$$

because $r(e_H)$ is the identity in $Aut(N)$.
The identity relation of multiplication on the right is verified in the same way.
Finding the inverse involves solving an equation. Given (n, h), we need to find (n', h') such that

$$(n', h')(n, h) = (e_N, e_H).$$

The semidirect product is a group

We need to prove that multiplication in $N \rtimes H$ is associative and that the identity and inverses exist. The identity is obvious: if we set $e = (e_N, e_H)$, then

$$(e_N, e_H)(n, h) = (e_N \cdot r(e_H)(n), e_H \cdot h)) = (e_N \cdot n, e_H \cdot h) = (n, h)$$

because $r(e_H)$ is the identity in $Aut(N)$.
The identity relation of multiplication on the right is verified in the same way.
Finding the inverse involves solving an equation. Given (n, h), we need to find (n', h') such that

$$(n', h')(n, h) = (e_N, e_H).$$

The semidirect product is a group

Now if

$$(e_N, e_H) = (n', h')(n, h) = (n' \cdot r(h')n, h' \cdot h)$$

then we must have $h' = h^{-1}$. So the equation we need to solve is

$$n' \cdot r(h^{-1})(n) = e_N; \;\; n' = (r(h^{-1})n)^{-1}$$

and this gives the solution. You can check that

$$(n, h)((r(h^{-1})n)^{-1}, h^{-1}) = (e_N, e_H)$$

as well.

The semidirect product is a group

Now if

$$(e_N, e_H) = (n', h')(n, h) = (n' \cdot r(h')n, h' \cdot h)$$

then we must have $h' = h^{-1}$. So the equation we need to solve is

$$n' \cdot r(h^{-1})(n) = e_N; \;\; n' = (r(h^{-1})n)^{-1}$$

and this gives the solution. You can check that

$$(n, h)((r(h^{-1})n)^{-1}, h^{-1}) = (e_N, e_H)$$

as well.

The semidirect product is associative

This is a calculation:

$$\begin{aligned}[(n_1,h_1)(n_2,h_2)](n_3,h_3) &= (n_1\cdot r(h_1)(n_2), h_1\cdot h_2)(n_3,h_3)\\ &= (n_1\cdot r(h_1)(n_2)\cdot r(h_1\cdot h_2)n_3, h_1h_2h_3).\end{aligned}$$

On the other hand

$$\begin{aligned}(n_1,h_1)[(n_2,h_2)(n_3,h_3)] &= (n_1,h_1)(n_2\cdot r(h_2)(n_3), h_2\cdot h_3)\\ &= (n_1\cdot r(h_1)(n_2\cdot r(h_2)(n_3)), h_1h_2h_3)\end{aligned}$$

So we need to check

$$n_1\cdot r(h_1)(n_2)\cdot r(h_1\cdot h_2)n_3 = n_1\cdot r(h_1)(n_2\cdot r(h_2)(n_3))$$

or even $r(h_1)(n_2)\cdot r(h_1\cdot h_2)n_3 = r(h_1)(n_2\cdot r(h_2)(n_3))$.

The semidirect product is associative

This is a calculation:

$$\begin{aligned}[(n_1, h_1)(n_2, h_2)](n_3, h_3) &= (n_1 \cdot r(h_1)(n_2), h_1 \cdot h_2)(n_3, h_3) \\ &= (n_1 \cdot r(h_1)(n_2) \cdot r(h_1 \cdot h_2)n_3, h_1 h_2 h_3).\end{aligned}$$

On the other hand

$$\begin{aligned}(n_1, h_1)[(n_2, h_2)(n_3, h_3)] &= (n_1, h_1)(n_2 \cdot r(h_2)(n_3), h_2 \cdot h_3) \\ &= (n_1 \cdot r(h_1)(n_2 \cdot r(h_2)(n_3), h_1 h_2 h_3)\end{aligned}$$

So we need to check

$$n_1 \cdot r(h_1)(n_2) \cdot r(h_1 \cdot h_2)n_3 = n_1 \cdot r(h_1)(n_2 \cdot r(h_2)(n_3)$$

or even $r(h_1)(n_2) \cdot r(h_1 \cdot h_2)n_3 = r(h_1)(n_2 \cdot r(h_2)(n_3)$.

The semidirect product is associative

This is a calculation:

$$\begin{aligned}[(n_1, h_1)(n_2, h_2)](n_3, h_3) &= (n_1 \cdot r(h_1)(n_2), h_1 \cdot h_2)(n_3, h_3) \\ &= (n_1 \cdot r(h_1)(n_2) \cdot r(h_1 \cdot h_2)n_3, h_1 h_2 h_3).\end{aligned}$$

On the other hand

$$\begin{aligned}(n_1, h_1)[(n_2, h_2)(n_3, h_3)] &= (n_1, h_1)(n_2 \cdot r(h_2)(n_3), h_2 \cdot h_3) \\ &= (n_1 \cdot r(h_1)(n_2 \cdot r(h_2)(n_3), h_1 h_2 h_3)\end{aligned}$$

So we need to check

$$n_1 \cdot r(h_1)(n_2) \cdot r(h_1 \cdot h_2)n_3 = n_1 \cdot r(h_1)(n_2 \cdot r(h_2)(n_3)$$

or even $r(h_1)(n_2) \cdot r(h_1 \cdot h_2)n_3 = r(h_1)(n_2 \cdot r(h_2)(n_3)$.

The semidirect product is associative, end of the calculation

We need to show

$$r(h_1)(n_2) \cdot r(h_1 \cdot h_2)n_3 = r(h_1)(n_2 \cdot r(h_2)(n_3))$$

But $r(h_1 \cdot h_2)n_3 = r(h_1)(r(h_2)(n_3))$ by the definition of $r : H \rightarrow Aut(N)$. And for any n, n',

$$r(h_1)(n) \cdot r(h_1)(n') = r(h_1)(n \cdot n')$$

because $r(h_1)$ is an automorphism. So

$$r(h_1)(n_2) \cdot r(h_1 \cdot h_2)n_3 = r(h_1)(n_2) \cdot r(h_1)(r(h_2)(n_3)) = r(h_1)(n_2 \cdot r(h_2)(n_3))$$

which is what we needed to prove.

The semidirect product is associative, end of the calculation

We need to show

$$r(h_1)(n_2) \cdot r(h_1 \cdot h_2)n_3 = r(h_1)(n_2 \cdot r(h_2)(n_3))$$

But $r(h_1 \cdot h_2)n_3 = r(h_1)(r(h_2)(n_3))$ by the definition of $r : H \to Aut(N)$. And for any n, n',

$$r(h_1)(n) \cdot r(h_1)(n') = r(h_1)(n \cdot n')$$

because $r(h_1)$ is an automorphism. So

$$r(h_1)(n_2) \cdot r(h_1 \cdot h_2)n_3 = r(h_1)(n_2) \cdot r(h_1)(r(h_2)(n_3)) = r(h_1)(n_2 \cdot r(h_2)(n_3))$$

which is what we needed to prove.

The semidirect product is associative, end of the calculation

We need to show

$$r(h_1)(n_2) \cdot r(h_1 \cdot h_2)n_3 = r(h_1)(n_2 \cdot r(h_2)(n_3))$$

But $r(h_1 \cdot h_2)n_3 = r(h_1)(r(h_2)(n_3))$ by the definition of $r : H \to Aut(N)$. And for any n, n',

$$r(h_1)(n) \cdot r(h_1)(n') = r(h_1)(n \cdot n')$$

because $r(h_1)$ is an automorphism. So

$$r(h_1)(n_2) \cdot r(h_1 \cdot h_2)n_3 = r(h_1)(n_2) \cdot r(h_1)(r(h_2)(n_3)) = r(h_1)(n_2 \cdot r(h_2)(n_3))$$

which is what we needed to prove.

Examples of semidirect products

Example

Recall that if p is prime, then $\mathrm{Aut}(\mathbb{Z}_p) = \mathbb{Z}_p^\times$*. So there is a semidirect product*

$$\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$$

of order $p(p-1)$ *for any p. It is non-commutative:*

$$x \cdot a = a \cdot ax, x \in \mathbb{Z}_p, a \in \mathbb{Z}_p^\times.$$

In this way we obtain new non-commutative groups of order $5 \cdot 4 = 20$, $7 \cdot 6 = 42$, *and so on. (When* $p = 3$ *we just get* D_6 *again).*

Examples of semidirect products

Example

Recall that if p is prime, then $Aut(\mathbb{Z}_p) = \mathbb{Z}_p^\times$. *So there is a semidirect product*

$$\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$$

of order $p(p-1)$ *for any p. It is non-commutative:*

$$x \cdot a = a \cdot ax, x \in \mathbb{Z}_p, a \in \mathbb{Z}_p^\times.$$

In this way we obtain new non-commutative groups of order $5 \cdot 4 = 20$, $7 \cdot 6 = 42$, *and so on. (When* $p = 3$ *we just get* D_6 *again).*

Examples of semidirect products

There are more possibilities. It is known that $\mathbb{Z}_p^\times$ is always a cyclic group. When $p = 7$ or $p = 11$ this follows from the classification of abelian groups: the only abelian groups of order 6 or 10 are $\mathbb{Z}_2 \times \mathbb{Z}_3$ or $\mathbb{Z}_2 \times \mathbb{Z}_5$, which are cyclic. .

So for example, $\mathbb{Z}_7^*$ contains a cyclic group C_3 of order 3, and the inclusion

$$C_3 \hookrightarrow \mathbb{Z}_7^* \xrightarrow{\sim} Aut(\mathbb{Z}_7)$$

gives us a semidirect product

$$\mathbb{Z}_7 \rtimes C_3$$

of order $7 \cdot 3 = 21$. Similarly $C_5 \subset \mathbb{Z}_{11}^\times$ gives us a semidirect product

$$\mathbb{Z}_{11} \rtimes C_5$$

of order 55.

Examples of semidirect products

There are more possibilities. It is known that $\mathbb{Z}_p^\times$ is always a cyclic group.When $p = 7$ or $p = 11$ this follows from the classification of abelian groups: the only abelian groups of order 6 or 10 are $\mathbb{Z}_2 \times \mathbb{Z}_3$ or $\mathbb{Z}_2 \times \mathbb{Z}_5$, which are cyclic. .

So for example, $\mathbb{Z}_7^*$ contains a cyclic group C_3 of order 3, and the inclusion

$$C_3 \hookrightarrow \mathbb{Z}_7^* \xrightarrow{\sim} Aut(\mathbb{Z}_7)$$

gives us a semidirect product

$$\mathbb{Z}_7 \rtimes C_3$$

of order $7 \cdot 3 = 21$. Similarly $C_5 \subset \mathbb{Z}_{11}^\times$ gives us a semidirect product

$$\mathbb{Z}_{11} \rtimes C_5$$

of order 55.

Examples of semidirect products

There are more possibilities. It is known that $\mathbb{Z}_p^\times$ is always a cyclic group.When $p = 7$ or $p = 11$ this follows from the classification of abelian groups: the only abelian groups of order 6 or 10 are $\mathbb{Z}_2 \times \mathbb{Z}_3$ or $\mathbb{Z}_2 \times \mathbb{Z}_5$, which are cyclic. .
So for example, $\mathbb{Z}_7^*$ contains a cyclic group C_3 of order 3, and the inclusion

$$C_3 \hookrightarrow \mathbb{Z}_7^* \xrightarrow{\sim} Aut(\mathbb{Z}_7)$$

gives us a semidirect product

$$\mathbb{Z}_7 \rtimes C_3$$

of order $7 \cdot 3 = 21$. Similarly $C_5 \subset \mathbb{Z}_{11}^\times$ gives us a semidirect product

$$\mathbb{Z}_{11} \rtimes C_5$$

of order 55.

Internal vs. external semidirect products

The construction above begins with two groups N and H and constructs a semidirect product $G = N \rtimes H$ with N as normal subgroup.

We can also start with a group G containing a normal subgroup N and a subgroup H.

Proposition

Suppose

1. $H \cdot N = G$ *and*
2. $H \cap N = \{e\}$

Then $G \xrightarrow{\sim} N \rtimes H$*, where* $r : H \to Aut(N)$ *is defined by*

$$r(h)(n) = hnh^{-1}.$$

Internal vs. external semidirect products

The construction above begins with two groups N and H and constructs a semidirect product $G = N \rtimes H$ with N as normal subgroup.

We can also start with a group G containing a normal subgroup N and a subgroup H.

Proposition

Suppose

1. $H \cdot N = G$ *and*
2. $H \cap N = \{e\}$

Then $G \xrightarrow{\sim} N \rtimes H$*, where* $r : H \to Aut(N)$ *is defined by*

$$r(h)(n) = hnh^{-1}.$$

Internal vs. external semidirect products

The construction above begins with two groups N and H and constructs a semidirect product $G = N \rtimes H$ with N as normal subgroup.
We can also start with a group G containing a normal subgroup N and a subgroup H.

Proposition

Suppose

1. $H \cdot N = G$ *and*
2. $H \cap N = \{e\}$

Then $G \xrightarrow{\sim} N \rtimes H$, *where* $r : H \to Aut(N)$ *is defined by*

$$r(h)(n) = hnh^{-1}.$$

Internal vs. external semidirect products

The construction above begins with two groups N and H and constructs a semidirect product $G = N \rtimes H$ with N as normal subgroup.
We can also start with a group G containing a normal subgroup N and a subgroup H.

Proposition

Suppose

1. $H \cdot N = G$ *and*
2. $H \cap N = \{e\}$

Then $G \xrightarrow{\sim} N \rtimes H$, *where* $r : H \to Aut(N)$ *is defined by*

$$r(h)(n) = hnh^{-1}.$$

Internal vs. external semidirect products

The construction above begins with two groups N and H and constructs a semidirect product $G = N \rtimes H$ with N as normal subgroup.
We can also start with a group G containing a normal subgroup N and a subgroup H.

Proposition

Suppose

1. $H \cdot N = G$ *and*
2. $H \cap N = \{e\}$

Then $G \xrightarrow{\sim} N \rtimes H$*, where* $r : H \to Aut(N)$ *is defined by*

$$r(h)(n) = hnh^{-1}.$$

Internal vs. external semidirect products, proof of the proposition

The proof is easy. We define a homomorphism $u : G \to N \rtimes H$ by setting

$$u(g) = (n, h) \text{ if } g = nh.$$

Every g can be written as a product $g = nh$ because $H \cdot N = G$. Moreover, this expression is unique, because $H \cap N = \{e\}$. So the map from G to $N \rtimes H$ is well-defined. It remains to be proved that it is a homomorphism: We write $g_1 = n_1 h_1$, $g_2 = n_2 h_2$. We have

$$u(g_1 g_2) = u(n_1 h_1 n_2 h_2) = u(n_1 [h_1 n_1 h_1^{-1}] h_1 h_2) = (n_1 [h_1 n_2 h_1^{-1}], h_1 h_2).$$

On the other hand,

$$u(g_1) u(g_2) = (n_1, h_1)(n_2, h_2) = (n_1 r(h_1)(n_2), h_1 h_2) = (n_1 [h_1 n_2 h_1^{-1}], h_1 h_2).$$

Internal vs. external semidirect products, proof of the proposition

The proof is easy. We define a homomorphism $u : G \to N \rtimes H$ by setting

$$u(g) = (n, h) \text{ if } g = nh.$$

Every g can be written as a product $g = nh$ because $H \cdot N = G$. Moreover, this expression is unique, because $H \cap N = \{e\}$. So the map from G to $N \rtimes H$ is well-defined. It remains to be proved that it is a homomorphism: We write $g_1 = n_1 h_1$, $g_2 = n_2 h_2$. We have

$$u(g_1 g_2) = u(n_1 h_1 n_2 h_2) = u(n_1 [h_1 n_1 h_1^{-1}] h_1 h_2) = (n_1 [h_1 n_2 h_1^{-1}], h_1 h_2).$$

On the other hand,

$$u(g_1)u(g_2) = (n_1, h_1)(n_2, h_2) = (n_1 r(h_1)(n_2), h_1 h_2) = (n_1 [h_1 n_2 h_1^{-1}], h_1 h_2).$$

Internal vs. external semidirect products, proof of the proposition

The proof is easy. We define a homomorphism $u : G \to N \rtimes H$ by setting

$$u(g) = (n, h) \text{ if } g = nh.$$

Every g can be written as a product $g = nh$ because $H \cdot N = G$.
Moreover, this expression is unique, because $H \cap N = \{e\}$.
So the map from G to $N \rtimes H$ is well-defined. It remains to be proved that it is a homomorphism: We write $g_1 = n_1h_1$, $g_2 = n_2h_2$. We have

$$u(g_1g_2) = u(n_1h_1n_2h_2) = u(n_1[h_1n_1h_1^{-1}]h_1h_2) = (n_1[h_1n_2h_1^{-1}], h_1h_2).$$

On the other hand,

$$u(g_1)u(g_2) = (n_1, h_1)(n_2, h_2) = (n_1r(h_1)(n_2), h_1h_2) = (n_1[h_1n_2h_1^{-1}], h_1h_2).$$

Internal vs. external semidirect products, proof of the proposition

The proof is easy. We define a homomorphism $u : G \to N \rtimes H$ by setting

$$u(g) = (n,h) \text{ if } g = nh.$$

Every g can be written as a product $g = nh$ because $H \cdot N = G$.
Moreover, this expression is unique, because $H \cap N = \{e\}$.
So the map from G to $N \rtimes H$ is well-defined. It remains to be proved that it is a homomorphism: We write $g_1 = n_1h_1$, $g_2 = n_2h_2$. We have

$$u(g_1g_2) = u(n_1h_1n_2h_2) = u(n_1[h_1n_1h_1^{-1}]h_1h_2) = (n_1[h_1n_2h_1^{-1}], h_1h_2).$$

On the other hand,

$$u(g_1)u(g_2) = (n_1,h_1)(n_2,h_2) = (n_1r(h_1)(n_2), h_1h_2) = (n_1[h_1n_2h_1^{-1}], h_1h_2).$$