Math 493 Lecture 15

Professor Andrew Snowden

Transcribed by Thomas Cohn

10/28/19

Let G be a group.

Recall: for $A, B \subset G$ subsets, $AB = \{ab \mid a \in A, b \in B\}$. If A and B are subgroups, then AB is not always a subgroup. However, if A is normal, then AB is a subgroup.

Recall:
Defn: G is the **(internal) direct product** of subgroups A and B if

1. A and B are normal
2. $AB = G$
3. $A \cap B = \{1\}$

Notation: $G = A \times B$

Defn: G is the **(internal) semi-direct product** of subgroups A and B if

1. A is normal
2. $AB = G$
3. $A \cap B = \{1\}$

Notation: $G = A \rtimes B$

Ex:

1. $G = M$, the group of rigid motions of the plane $P = \mathbb{R}^2$.
   A is the group of translations.
   B is $\mathrm{O}(2)$, the group of origin-preserving transformations.
   $G = A \rtimes B$.

2. $G = D_n$, the dihedral group of order $2n$.
   A is the group of rotations ($\mathrm{ord}(A) = n$).
   B is the subgroup generated by any reflection.
   $G = A \rtimes B$.

3. $G = \mathrm{O}(n)$.
   $A = \mathrm{SO}(n)$.
   B is the subgroup generated by any reflection.
   $G = A \rtimes B$.

4. $G = A \times B$.
   $A = A$.
   $B = B$.
   $G = A \rtimes B$. (I.e. every direct product is a semi-direct product.)

So, among other things, we have $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = D_n$. Thus, we cannot recover G from A and B as an abstract group from a semi-direct product.

Let X be a set. $\mathrm{Perm}(X)$ is the group of permutations of X, i.e., the set of all bijections $X \to X$, under composition.
$S_n = \mathrm{Perm}(\{1, \dots, n\})$.

If X is a G-set, then for $g \in G$, we get a permutation of X by $\begin{array}{c} X \to X \\ x \mapsto gx \end{array}$.
This defines a function $G \to \mathrm{Perm}(X)$, which is a group homomorphism. In fact, giving an action of G on X is the same as giving a homomorphism $G \to \mathrm{Perm}(X)$.

Defn: Now, say X is a group. $\mathrm{Aut}(X) \subseteq \mathrm{Perm}(X)$. If G acts on X, we say G **acts by group homomorphisms** if the map $G \to \mathrm{Perm}(X)$ lands in $\mathrm{Aut}(X)$.

Explicitly, this means $g \in G, x, y \in X \Rightarrow g \cdot (xy) = (g \cdot x)(g \cdot y)$.

Ex:

1. G acts on itself by left-multiplication. This action *is not* by group homomorphisms.
2. G acts on itself by conjugation. This action *is* by group homomorphisms.

Say $G = A \rtimes B$. Given $b \in B$, we know that conjugation by b is a group homomorphism $G \to G$, and maps A to itself because A is normal. Let

$$\begin{aligned} \varphi_b : A &\to A \\ a &\mapsto bab^{-1} \end{aligned}$$

Then $\varphi_b \in \mathrm{Aut}(A)$. The function

$$\begin{aligned} \varphi : B &\to \mathrm{Aut}(A) \\ b &\mapsto \varphi_b \end{aligned}$$

is a group homomorphism. Reason: $\varphi_{bb'}(a) = bb'a(bb')^{-1} = b(b'a(b')^{-1})b^{-1} = \varphi_b(\varphi_{b'}(a))$.

Note: Every element of G can be written *uniquely* as ab with $a \in A$ and $b \in B$.
Existence is clear – we just need to check uniqueness.
Say $ab = a'b'$. Then $1 = (a')^{-1}a = b'b^{-1} \in A \cap B = \{1\}$. So $a = a'$ and $b = b'$, because inverses are unique.

To rephrase, the function $\begin{array}{c} A \times B \to G \\ (a, b) \mapsto ab \end{array}$ is a bijection of sets. But in general, it *is not* a group homomorphism.

How do we multiply elements of G under this description?

$$(ab)(a'b') = (aba'b^{-1})(bb') = (a\varphi_b(a'))(bb')$$

Defn: A and B are two groups. $\varphi : B \to \mathrm{Aut}(A)$ is a group homomorphism. The **(external) semi-direct product** of A and B is the set of elements in $A \times B$, with multiplication
$(a, b)(a', b') = (a\varphi_b(a'), bb')$. Notation: $G = A \rtimes_\varphi B$ (the subscript is optional).

Suppose $G = A \rtimes B$. We've constructed $\varphi : B \to \mathrm{Aut}(A)$.

From the above discussion, we know $G \cong A \rtimes_\varphi B$ (external). So internal semi-direct products are external semi-direct products.

Now, say $G = A \rtimes_\varphi B$ (external). Then $\bar{A} = \{(a, 1) \mid a \in A\}$, $\bar{B} = \{(1, b) \mid b \in B\}$. $\bar{A}, \bar{B} \subseteq G$. We claim $\bar{A}$ and $\bar{B}$ are subgroups of G, and G is the internal semi-direct product.

Proof:
$\bar{A}$ is closed under multiplication: $(a,1)(a',1) = (a\varphi_1(a'), 1\cdot 1) = (aa',1)$, because $\varphi_1 = \mathrm{Id}_A$, so $\bar{A} \cong A$.
$\bar{B}$ is closed under multiplication: $(1,b)(1,b') = (1\varphi_b(1), bb') = (1,bb')$, so $\bar{B} \cong B$.
$G = \bar{A}\bar{B}$: $(a,1)(1,b) = (a\varphi_1(1), 1\cdot b) = (a,b)$.
$\bar{A}$ normal: $(1,b)(a,1)(1,b)^{-1} = (1,b)(a,1)(1,b^{-1}) = (1,b)(a,b^{-1}) = (\varphi_b(a), bb^{-1}) = (\varphi_b(a),1) \in \bar{A}$. $\square$

Ex: Some external semi-direct products:

1. $\varphi : B \to \mathrm{Aut}(A)$ is the trivial homomorphism. Then $\varphi_b = \mathrm{Id}_A$, $\forall b$, so $\varphi_b(a) = a$, $\forall a, b$. Then $(a,b)(a',b') = (a\varphi_b(a'), bb') = (aa', bb')$. So we get the direct product $A \times B$.

2. $G = D_n$, A is the group of rotations $\left\langle \rho_{\frac{2\pi}{n}} \right\rangle \cong \mathbb{Z}/n\mathbb{Z}$. B is the group generated by some reflection, which is equal to $\langle r \rangle \cong \mathbb{Z}/2\mathbb{Z}$. We want to understand

$$\begin{aligned} \varphi : B &\to \mathrm{Aut}(A) \\ 1 &\mapsto \mathrm{Id}_A \\ r &\mapsto (\rho^k \mapsto \rho^{-k}) \end{aligned}$$

   Recall, $r\rho^k r^{-1} = \rho^{-k}$, so we have

$$\rho^k \longleftarrow\!\shortmid\; k$$

$$\begin{tikzcd} \rho^k \arrow[d, mapsto] & \langle \rho \rangle \arrow[d, "\varphi_r"] & \mathbb{Z}/n\mathbb{Z} \arrow[l, "\sim"'] \arrow[d] & k \arrow[d, mapsto] \\ \rho^{-k} & \langle \rho \rangle & \mathbb{Z}/n\mathbb{Z} \arrow[l, "\sim"'] & -k \end{tikzcd}$$

3. F a field, $A = F^n$ (the group of column vectors, under addition). $B = \mathrm{GL}_n(F) \subseteq \mathrm{Aut}(A)$. ($B$ consists of F-linear automorphisms.)Take φ to be inclusion. Explicitly, $\varphi_b(a) = ba$ (matrix multiplication).
   $G = A \rtimes_\varphi B$: $(a,b)(a',b') = (a + \varphi_b(a'), bb') = (a + ba', bb')$ (with vector addition, and matrix multiplication).

Let $A \lhd G$ a normal subgroup. Let A' be some nonzero proper F-subspace of A. $A' \lhd A$, but $A' \ntriangleleft G$.

Question: What is $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$?
Suppose $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is an automorphism. φ is determined by $\varphi(1)$, call this $a \in \mathbb{Z}/n\mathbb{Z}$.
$\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = a + a = 2a$.
$\varphi(3) = \varphi(2+1) = \varphi(2) + \varphi(1) = 2a + a = 3a$.
In general, $\varphi(k) = ka$ (multiplication modulo n). Since φ is an automorphism, $\exists k$ s.t. $\varphi(k) = 1$, so $ka = 1$.
So a is invertible under multiplication.

Defn: We say a is a **unit** of $\mathbb{Z}/n\mathbb{Z}$.

$(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of units of $\mathbb{Z}/n\mathbb{Z}$, and it is a group under multiplication.

Summary: The map $\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^\times &\to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \\ a &\mapsto m_a = \text{multiplication by } a \end{aligned}$ is an isomorphism of groups.
Note: $m_a(m_b(x)) = a \cdot b \cdot x = m_{ab}(x)$, so $m_a \circ m_b = m_{ab}$, so this is a group homomorphism.)

Lemma: If $a \in \mathbb{Z}/n\mathbb{Z}$, then a is a unit iff $\gcd(a,n) = 1$.

Ex:

- If $n = p$ is prime, $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{F}_p^\times = \mathbb{F} \setminus \{0\}$. We've shown this is cyclic, and of order $p - 1$.
- $(\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\} \cong \mathbb{Z}/2\mathbb{Z}$.
- $(\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\} \cong \mathbb{Z}/2\mathbb{Z}$.
- $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- $(\mathbb{Z}/16\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Ex: The last computation implies we have an injective group homomorphism $\varphi : \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/16\mathbb{Z})$. We get a semi-direct product $\mathbb{Z}/16\mathbb{Z} \rtimes_\varphi \mathbb{Z}/4\mathbb{Z}$.