Math 120 WIM

Ann He

2017

1. Definition of Semiproduct

Given the groups H and K, and given the homomorphism φ from K into the automorphism group of H, $\varphi : K \to Aut(H)$, we can define a new group $G = H \rtimes K$ whose elements are (h, k) with $h \in H$ and $k \in K$ where the product of elements in G is defined as

$$(h_1, k_1)(h_2, k_2) = (h_1\varphi_{k_1}(h_2), k_1k_2)$$

Here, $\varphi_{k_1}(h_2)$ can be thought of as $k_1 \in K$ acting on $h_2 \in H$. Since $Aut(H) \leqslant S_H$, φ induces a group action of K on H.

First, we claim that for $k \in K$ and $x, y \in H$

$$\varphi_k(xy) = \varphi_k(x)\varphi_k(y)$$

This follows from the fact that φ_k is an automorphism of H.

Next, we claim that for $k_1, k_2 \in K$ and $x \in H$

$$\varphi_{k_1}(\varphi_{k_2}(x)) = \varphi_{k_1k_2}(x)$$

Since $Aut(H) \leqslant S_H$, $Aut(H)$ is a group under composition (product) of permutations, the above claim holds.

Now, verify associativity in G given the above definition of multiplication.

$$\begin{aligned}(h_1, k_1)((h_2, k_2)(h_3, k_3)) &= (h_1, k_1)(h_2\varphi_{k_2}(h_3), k_2k_3) = (h_1\varphi_{k_1}(h_2\varphi_{k_2}(h_3)), k_1k_2k_3)\\ &= (h_1\varphi_{k_1}(h_2)\varphi_{k_1}(\varphi_{k_2}(h_3)), k_1k_2k_3)\\ &= (h_1\varphi_{k_1}(h_2)\varphi_{k_1k_2}(h_3), k_1k_2k_3)\\ &= (h_1\varphi_{k_2}(h_2), k_1k_2)(h_3, k_3) = ((h_1, k_1)(h_2, k_2))(h_3, k_3)\end{aligned}$$

Let (h, k) be any element of G. Then

$$(e_H, e_K)(h, k) = (e_H\varphi_{e_K}(h), e_Kk) = (e_Hh, e_Kk) = (he_H, ke_K) = (h\varphi_k(e_H), ke_K) = (h, k)(e_H, e_K) = (h, k)$$

Where we know that $\varphi_k(e_H) = 1$ by the following verification

$$\varphi_k(e_H) = \varphi_k(e_He_H) = \varphi_k(e_H)\varphi_k(e_H)$$

Left cancellation yielding

$$1 = \varphi_k(e_H)$$

Finally, we claim that the inverse of (h, k) is $(\varphi_{k^{-1}}(h^{-1}), k^{-1})$. We verify

$$(h, k)(\varphi_{k^{-1}}(h^{-1}), k^{-1}) = (h\varphi_k(\varphi_{k^{-1}}(h^{-1})), kk^{-1}) = (h\varphi_{kk^{-1}}(h^{-1}), e_K) = (e_H, e_K)$$

and

$$(\varphi_{k^{-1}}(h^{-1}), k^{-1})(h, k) = (\varphi_{k^{-1}}(h^{-1})\varphi_{k^{-1}}(h), k^{-1}k) = (\varphi_{k^{-1}}(h^{-1}h), e_K) = (e_H, e_K)$$

Concluding that G is a group.

2

Fact: Let G be a finite group, H be a normal subgroup in G, and K a subgroup of G such that $HK = G$ and $H \cap K = \{e\}$. Then G is isomorphic to a semiproduct of H and K.

Proof: Let $\varphi : K \to Aut(H)$ be the homomorphism which maps k to the automorphism of left conjugation by k on H such that $\varphi_k(h) = khk^{-1}$.

We know that $G = HK$ so that every element in G can be represented as some hk, $h \in H$, $k \in K$. To prove that this representation is unique suppose $h_1k_1 = h_2k_2$. Then, $h_1h_2^{-1} = k_2k_1^{-1}$ where $h_3 = h_1h_2^{-1} \in H \cap K$ implying $h_1h_2^{-1} = e$, so that $h_1 = h_2$. The same argument applies for k_1 and k_2.

Now that we know $g \in G$ can be unique represented as the product of some $h \in H$ and $k \in K$, define the map $\Psi : HK \to H \rtimes K$ with $\Psi(hk) = (h, k)$. Define $\bar{G} = \{(h, k)|h \in H, k \in K\}$. Let G be the semiproduct group with φ the map of left conjugation, as defined above. We will now prove that Ψ is an isomorphism.

Since hk is a unique representation of G, Ψ is well-defined. To check that it is a homomorphism let $h_3 = k_1h_2k_1^{-1}$ and consider:

$$\Psi(h_1k_1h_2k_2) = \Psi(h_1k_1h_2(k_1^{-1}k_1^{1})k_2) = \Psi(h_1h_3k_1k_2) = (h_1h_3, k_1k_2) = (h_1, k_1)(h_2, k_2) = \Psi(h_1k_1)\Psi(h_2k_2).$$

Since $|G| = |HK| = \dfrac{|H||K|}{|H \cap K|} = |H||K|$ the two sets are equal in size. Furthermore, Ψ is surjective since any element (h, k) with h from H and k from K. Thus, the homomorphism is an isomorphism.

3. Preliminary propositions

Proposition 1. Let Z_n denote the cyclic group of order n. Then $Aut(Z_n) \cong (\mathbb{Z}/n\mathbb{Z})^{\times}$.

Proof: Let x be a generator for Z_n. Let $\varphi \in Aut(Z_n)$. As φ is an isomorphism from Z_n to itself, $\varphi(x) = x^a$ for some $a \in \{1, ..., n\}$. Note that this determines φ since any $y \in Z_n$ can be written as x^i for $i \in \{1, ..., n\}$ so that $\varphi(y) = \varphi(x^i) = \varphi(x)^i = x^{ai}$. Since $|x| = n$, a is considered modulo n. Since φ preserves element orders, $|x| = |\varphi(x)| = |x^a| = n$, implying x^a also generates Z_n so that $(a, n) = 1$. Then, for every such a^*, we have a map φ which sends to x to x^{a^*}. By definition there are exactly $\varphi(n)$ such a^*'s, with $\{a^*\}$ being the elements of $(\mathbb{Z}/n\mathbb{Z})^x$. Denote $\varphi(x) = x^{a^*}$ as φ_{a^*}. We then map φ_{a^*} to $a^* \in (\mathbb{Z}/n\mathbb{Z})^x$. As per the previous comments, this map is surjective and injective. Name this map Ψ. We will prove that it is a homomorphism, from which we deduce that $Aut(Z_n) \cong (\mathbb{Z}/n\mathbb{Z})^x$. Let $\varphi_a, \varphi_b \in Aut(Z_n)$.

First note that for $\varphi_a, \varphi_b \in Aut(Z_n)$,

$$\varphi_a \circ \varphi_b(x) = \varphi_a(\varphi_b(x)) = \varphi_a(x^b) = x^{ab} = \varphi_{ab}(x)$$

so that

$$\Psi(\varphi_a \circ \varphi_b) = \Psi(\varphi_{ab}) = ab(\mathrm{mod} n) = (a(\mathrm{mod} n) * b(\mathrm{mod} n)) = \Psi_{\varphi_a}\Psi_{\varphi_b}$$

Where the last equality holds because a and b for $\varphi_a, \varphi_b \in Aut(Z_n)$ are such that $a < n, b < n$ so $a = a(\mathrm{mod} n)$ and $b = b(\mathrm{mod} b)$.

Proposition 2. $Aut(Z_2 \times Z_2) \cong S_3$.

Proof: Any isomorphism from $Z_2 \times Z_2$ to itself must fix e since isomorphisms preserve element orders. Since any non-identity element has order 2, $\varphi \in Aut(Z_2 \times Z_2)$ is free to permute the non-identity elements among each other. There are 3 non-identity elements of $Z_2 \times Z_2$, so $Aut(Z_2 \times Z_2)$ is naturally isomorphic to S_3.

Proposition 3. Let G be a group. If $|G| = 12$, then $n_3 = 1$ or $n_2 = 1$.

Proof: From Sylow's theorem, we know that $n_3 \in \{1, 4\}$ and $n_2 = 1, 3$. Suppose $n_3 = 4$, we will show that $n_2 = 1$. Denote the four distinct Sylow-3 groups of G P_1, P_2, P_3 and P_4. They each have cardinality three and are isomorphic to Z_3. We claim that $P_i \cap P_j = 1$ for $i \neq j$. To see this, suppose for a contradiction that $x \in P_i \cap P_j$ such that $x \neq 1$ and $i \neq j$. Then x must be a generator P_i since it is a non-identity element of a group of prime order, so $\langle x \rangle = P_i$. But this also holds for P_j so $P_i = P_j$, a contradiction. Then, the four Sylow-3 groups give us a total of $2 \times 4 = 8$ elements of order 3.

Let Q_k denote a Sylow-2 group. We claim that $P_i \cap Q_k = 1$ for any i, k. Any non-identity element of P_i has order 3. But an order 3 element cannot belong to Q_k as per Lagrange's theorem.

There are $12 - 8 = 4$ elements in G which do not have order 3. Any Q_k has order 4, by Sylow's Theorem, so there is exactly one Q_k.

Proposition 4. Let G be a group such that $|G| = 4$. Then $G \cong Z_4$ or $G \cong Z_2 \times Z_2$.

Proof: Suppose $G \ncong Z_4$. By Lagrange's theorem any non-identity element of G has order 2 or 4. Let x be a non-identity element of G. $|x| \neq 4$ since if $|x| = 4$ then $Z_4 \cong \langle x \rangle = G$. Then x must have order 2. Since $|G| = 4$, there are 3 non-identity elements each of order 2 and one identity element. Let a, b, c denote the non-identity elements. We claim that any two of these multiplied together yields the third non-identity element. Without loss of generality consider the product ab. If $ab = a$ then $b = 1$, a contradiction. The same holds for $ab = b$, whereby we get $a = 1$, another contradiction. If $ab = 1$, then $a = b^{-1}$ but since b is order 2, the unique inverse of b is b, so this cannot be. then $ab = c$. Similarly, $ba = c$, $ac = ca = b$, and $bc = cb = a$. This group is isomorphic to Klein-4, which is isomorphic to the direct product $Z_2 \times Z_2$.

4. Classification of groups of order 12

Let G be a group such that $|G| = 12$. Let P be a Sylow-2 group of G and Q be a Sylow-3 group of G. Since $n_2 = 1$ or $n_3 = 1$, $P \trianglelefteq G$ or $Q \trianglelefteq G$. In the first case $G \cong P \rtimes Q$ for the unique Sylow-2 group P and some Sylow-3 group Q and in the latter case $G \cong Q \rtimes P$ for the unique Sylow-3 group Q and some Sylow-2 group P. We now use this result to classify groups of order 12.

Case 1: $P \trianglelefteq G$ and $P \cong Z_4$. $Aut(P) \cong Aut(Z_4) \cong (\mathbb{Z}/4\mathbb{Z})^{\times} \cong Z_2$. Since $Q \cong Z_3$ we need to determine all homomorphisms $\varphi : Z_3 \to Z_2$. We claim that φ must be trivial. Let $\langle x \rangle = Q$ and $\langle y \rangle = Z_2$. If $\varphi(x) = y$ then $\varphi(x^3) = \varphi(x)\varphi(x)\varphi(x) = y$ but $\varphi(x^3) = \varphi(e) = e$, a contradiction. Similarly, if $\varphi(x^2) = y$, then $\varphi(x^4) = \varphi(x^2)\varphi(x^2) = e$ but then $\varphi(x^4) = \varphi(x) = e$ which implies $\varphi(x^2) = \varphi(x)\varphi(x) = e$, a contradiction. Then, φ is the trivial homomorphism and G is isomorphic to the direct product $Z_4 \times Z_3 \cong Z_{12}$, an abelian group since the direct product of abelian groups is abelian.

Case 2: $P \trianglelefteq G$ and $P \cong Z_2 \times Z_2$. Then $Aut(P) \cong Aut(Z_2 \times Z_2) \cong S_3$. We will now determine all homomorphisms $\varphi : Z_3 \to S_3$. If φ is the trivial homomorphism, then G is isomorphic to the direct product $Z_2 \times Z_2 \times Z_3$, an abelian group.

Let $\langle x \rangle = Q$. In order for φ to be nontrivial, it must send x to some $y \in S_3$ which is order 3. To see this let $\varphi(x) = y$. Then $e = \varphi(e) = \varphi(x^3) = \varphi(x)^3 = y^3$, which implies $|y| \mid 3$. By assumption $|y| \neq 1$, so $|y| = 3$. Then $\varphi(x) = y^i$ for $i = 1, 2$ ($i = 0$ gives us the trivial homomorphism). The only order 3 cyclic subgroup of S_3 is $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$. Then if φ is nontrivial, Q acts on P by permuting the non-identity elements of $P \cong Z_2 \times Z_2$. A group which fits this description is A_4, a non-abelian group, which contains the non-cyclic normal subgroup of order 4 $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

Case 3: $Q \trianglelefteq G$ and $P \cong Z_4$. Then $Aut(Q) = Aut(Z_3) \cong (\mathbb{Z}/3\mathbb{Z})^x \cong Z_2$. We will determine the homomorphisms $\varphi : Z_4 \to Z_2$. In the case that φ is trivial, G is isomorphic to the direct product $Z_3 \times Z_4 \cong Z_{12}$, which is abelian.

Let $P = \langle x \rangle$ and $Z_2 = \langle y \rangle$. In the case that $\varphi(x) = y$, we have the semidirect product of the form

$$(a, b)(c, d) = (a\varphi_b(c), bd)$$

where $\varphi_b(c) = c$ if $x^2, e = b$ and $\varphi_b(c) = c^{-1}$ if $x^3, x = b$. Then $G \cong Z_3 \rtimes Z_4 \ncong Z_{12}$, and is non-abelian.

Case 4: $Q \trianglelefteq G$ and $P \cong Z_2 \times Z_2$ We are interested in the homomorphisms $\varphi : Z_2 \times Z_2 \to Z_2$. Let a, b, c denote the three non-identity elements of $Z_2 \times Z_2$ and let $Z_2 = \langle y \rangle$. Then nontrivial homomorphisms φ map two of a, b, c to y and the third to e. These isomorphic semidirect products are isomorphic to non-abelian D_{12} which contains the normal, cyclic Sylow-3 group $\{e, r^2, r^4\}$ and non-cyclic Sylow-2 group $\{e, r^3, s, sr^3\}$ isomorphic to V_4.