THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 3030 Abstract Algebra 2024-25
Tutorial 4
3rd October 2024

- Tutorial exercise would be uploaded to blackboard on Mondays provided that there is a tutorial class on that Thursday. You are not required to hand in the solution, but you are advised to try the problems before tutorial classes.
- Please send an email to echlam@math.cuhk.edu.hk if you have any questions.

1. Recall the definition of automorphism group, can you determine the automorphism groups of $\mathbb{Z}_p$ for prime p and $\mathbb{Z}$? (Bonus: How about automorphisms of $\mathbb{Z}^2$? Hint: think about linear maps.)
2. Suppose G is a finite group and $T \in \mathrm{Aut}(G)$ so that $Tg = g \Leftrightarrow g = e$, prove that every $h \in G$ can be expressed as $g^{-1}(Tg)$ for some g.
3. Suppose G is a finite group with $T \in \mathrm{Aut}(G)$, so that $Tg = g \Leftrightarrow g = e$. Suppose further that $T^2 = \mathrm{Id}$, show that G is abelian.
4. Find the centers for the dihedral group D_{2n}, the symmetry group of n-gon.
5. We have learnt about direct product of groups in the lectures as group structure defined on a new set $G_1 \times G_2$. It is possible to make sense of direct product internally within a group as follows.

   Suppose G is a group satisfying the following,

   (a) H, K are normal subgroups of G.
   (b) $H \cap K = \{e\}$.
   (c) $G = HK = \{hk \in G : h \in H, k \in K\}$

   Show that $G \cong H \times K$.

- If time permits, I will cover the following extra materials in the tutorial. Note that the extra materials would **NOT** appear in the midterm nor exam.

Notes on semidirect products

In the lectures, we have encountered two notions about constructing groups from smaller pieces. The first is direct product $H \times K$, which is formed by imposing no conditions on how elements of H, K interact. In other words, we set $hk = kh$ for any h, k. There is a second notion of a group extension that is more sophiscated. Whenever we have a short exact sequence,

$$1 \to H \to G \to K \to 1$$

i.e. an injective $\varphi_1 : H \to G$ and a surjective $\varphi_2 : G \to K$ together with the condition that $\mathrm{im}(\varphi_1) = \ker(\varphi_2)$. We say that G is extension of K by H. In this case, note that $H \cong \varphi(H) \cong \ker(\varphi_2)$ can be regarded as a normal subgroup of G, and by isomorphism theorem $K \cong G/\varphi_1(H)$. So in the case when H, K are finite, $|G| = |H| \cdot |K|$, and we think of H, K as building blocks of G. However, in general there is no good way of writing down the structure of G based on H, K.

Semidirect product is a middle ground between direct product and group extension. In Q6 above, one would obtain semidirect product when the condition H, K are normal subgroups is relaxed to just having H as a normal subgroup and K is a general subgroup. We use the notation $H \rtimes K$ or $K \ltimes H$ to denote semidirect products (note that this is not symmetric unlike direct product). One simple example is $G = S_3$, it is the semidirect product of the subgroups $H = \langle (123) \rangle$ and $K = \langle (12) \rangle$. Notice that K is not normal here, in particular generally we won't have the property that $hk = kh$ like we had for direct products. For that reason, in general the isomorphism types of H, K alone is not enough to determine $H \rtimes K$, we need specific details of how they interact within a bigger group G as in the definition.

There is another way of describing the extra data by using automorphism group, which you can think of as describing the relation $hkh'k' = h''k''$ in $G = HK$. Define $\varphi : K \to \mathrm{Aut}(H)$ by $k \mapsto \varphi_k(h) = khk^{-1}$, one can check that this is a homomorphism. With this, we have for any $h, h' \in H$ and $k, k' \in K$,

$$hkh'k' = h(kh'k^{-1})kk' = h\varphi_k(h')kk' = h''k'',$$

$$\text{and } (hk)^{-1} = (k^{-1}h^{-1} = k^{-1}h^{-1}k)k^{-1} = \varphi_{k^{-1}}(h^{-1})k^{-1} \quad .$$

In other words, we can determine the structure of $H \rtimes K$ by the data of the map $K \to \mathrm{Aut}(H)$. Like the case for direct products, we can define semidirect products of H, K externally without starting from a bigger group G.

Theorem. Let H, K be groups and suppose we have a homomorphism $\varphi : K \to \mathrm{Aut}(H)$, then there is a group G so that we have embeddings $\iota_1 : H \hookrightarrow G$ and $\iota_2 : K \hookrightarrow G$ so that $G \cong \iota_1(H) \rtimes \iota_2(K)$.

Proof. Let $G = H \times K$ as sets, we can define the group operation on G by taking $(h, k) \cdot (h', k') := (h\varphi_k(h'), kk')$. Writing 1 as both the identities of H and K, we also have $(1, 1)$ is an identity of G since $(1, 1) \cdot (h, k) = (1 \cdot \varphi_1(h), 1 \cdot k) = (h, k)$ and similarly for right identity. We define the inverse of (h, k) by as $(h, k)^{-1} = (\varphi_{k^{-1}}(h^{-1}), k^{-1})$. Then $(h, k)^{-1} \cdot (h, k) =$

$(\varphi_{k^{-1}}(h^{-1})\varphi_{k^{-1}}(h), k^{-1}k) = (\varphi_{k^{-1}}(h^{-1}h), 1) = (1, 1)$ so left inverse exists, similarly one can verify for right inverse. I leave the proof of associativity of the group operation to the readers ;)

With G constructed, we have natural embeddings $H \to G$ by $\iota(h) = (h, 1)$ and $K \to G$ by $\iota_2(k) = (1, k)$. One can also verify that they are indeed injective homomorphisms (this is not by definition because we have a modified operation on $H \times K$!) First of all, $\iota_1(H) \triangleleft G$ because the second component of $(h, k) \cdot (x, 1) \cdot (h, k)^{-1}$ is simply given by $k \cdot 1 \cdot k^{-1} = 1$. Now $\iota_1(H) \cap \iota_2(K) = (1, 1)$, and $G = HK$ since any $(h, k) = (h, 1) \cdot (1, k) = (h\varphi_1(1), k)$. So we indeed have $G \cong \iota_1(H) \rtimes \iota_2(K)$ as claimed. ■

The notion of semidirect product may look weird at first. One can realize it as a twisted product between two groups. This generalizes direct product since direct product is just given by the trivial map $K \to \mathrm{Aut}(H)$ by $k \mapsto \mathrm{Id}$. There is yet another way to realize semidirect products as a restricted type of group extensions.

Theorem. Suppose $1 \to H \xrightarrow{\varphi} G \xrightarrow{\psi} K \to 1$ is an exact sequence that splits, i.e. there exists a homomorphism $s : K \to G$ so that $\psi \circ s = \mathrm{Id} : K \to K$. Then $G = \varphi(H) \rtimes s(K)$.

Proof. Recall that in any short exact sequence, $\varphi : H \to G$ is injective, and $\psi : G \to K$ is surjective. This forces $s : K \to G$ to be injective, since $s(k) = e \Rightarrow k = \psi(s(k)) = \psi(e) = e$. To show that G is the semidirect product of subgroups, we must show that:

1. $\varphi(H)$ is normal: This is true since $\varphi(H) = \ker(\psi)$.
2. $\varphi(H) \cap s(K) = \{e\}$: If $g = \varphi(h) = s(k)$, then $e = \psi(\varphi(h)) = \psi(g) = \psi(s(k)) = k$. Here the first equality is from exactness, and the last equality is from property of s. Therefore $g = s(k) = s(e) = e$.
3. $G = \varphi(H)s(K)$, in the finite case, we can simply see this by cardinality argument that $|G| = |\varphi(H)s(K)| = |\varphi(H)| \cdot |s(K)| = |H| \cdot |K|$, which is guaranteed by property of exact sequence. In general, given any $g \in G$, we can take $k = \psi(g)$. Note that $g \cdot s(k^{-1})$ is in $\varphi(H) = \ker(\psi)$ since $\psi(g) \cdot \psi(s(k^{-1})) = kk^{-1} = 1$. Therefore $g = gs(k^{-1}) \cdot s(k) \in \varphi(H)s(K)$.

This proves that $G = \varphi(H) \rtimes \psi(K)$. ■

One can also just construct a map $K \to \mathrm{Aut}(H)$. To simplify notation, let's not distinguish between $H \cong \varphi(H)$ as they are isomorphic. Then $\varphi_k : H \to H$ is defined simply by $\varphi_k(h) = s(k) \cdot h \cdot s(k)^{-1}$. Conversely, one can also construct a split exact sequence whenever we have $G \cong H \rtimes K$: as we can take $H \triangleleft G$, we have the sequence $1 \to H \to G \to G/H \to 1$. Here we can identify $K \cong G/H$ since $G = HK$ and the right cosets have multiplication given by $(Hk)(Hk') = H(kk')$ by property of semidirect product. Then the splitting is just given by inclusion $K \hookrightarrow G$ because $K \hookrightarrow G \to G/H$ is given by $k \mapsto 1 \cdot k \mapsto Hk$.

We end this section by discussing an example and a non-example of semidirect product. Consider the normal subgroup $SL(n, F) \leq GL(n, F)$ where F is an arbitrary field, this is normal as it is obtained from the kernel of the homomorphism $\det : GL(n, F) \to F^\times$, here $F^\times$

is the multiplicative group of the field. We also have $F^\times \leq GL(n, F)$ by

$$\iota : a \mapsto \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Clearly, $\det(\iota(a)) = a \in F^\times$, therefore $1 \to SL(n, F) \hookrightarrow GL(n, F) \overset{\det}{\to} F^\times \to 1$ is a split exact sequence, thus corresponding to a semidirect product. Alternatively, one can realize this semidirect product via conjugate action of $\iota(a)$, in other words $F^\times \to \mathrm{Aut}(SL(n, F))$ as given by $a \mapsto (A \mapsto \iota(a)A\iota(a)^{-1})$. Hence, we have $GL(n, F) \cong SL(n, F) \rtimes F^\times$.

For a non-example (a group extension that is not split), consider

$$1 \to \mathbb{Z}_p \to \mathbb{Z}_{p^2} \to \mathbb{Z}_p \to 1$$

Where the first map is given by $1 \mapsto p \in \mathbb{Z}_{p^2}$. Since $\mathbb{Z}_{p^2}$ is abelian, if we have a splitting $\mathbb{Z}_p \to \mathbb{Z}_{p^2}$, that would give two subgroups of $\mathbb{Z}_{p^2}$ that are isomorphic to $\mathbb{Z}_p$, which are necessarily normal. This would imply that $\mathbb{Z}_{p^2} \cong \mathbb{Z}_p^2$, which is a contradiction.