Math 761 Homework 2

Fall 2015 Drew Armstrong

Problem 1. Image and Preimage. Let $\varphi : G \to H$ be a group homomorphism and consider the Galois connection $\varphi : \mathscr{L}(G) \rightleftarrows \mathscr{L}(H) : \varphi^{-1}$ between image and preimage. Prove that for all subgroups $A \in \mathscr{L}(G)$ and $B \in \mathscr{L}(H)$ we have

- $\varphi^{-1}(\varphi(A)) = A \vee \ker\varphi$
- $\varphi(\varphi^{-1}(B)) = B \wedge \operatorname{im}\varphi$

Proof. Recall that in order to view $\varphi : \mathscr{L}(G) \rightleftarrows \mathscr{L}(H) : \varphi^{-1}$ as a Galois connection we will regard $\mathscr{L}(H)$ as partially ordered by **reverse-inclusion**. Then we can apply all of the results from the first homework.

First we will show that $\varphi^{-1}(\varphi(A)) = (A \vee \ker\varphi)$. By general nonsense we know that $\varphi^{-1} \circ \varphi$ is a closure operator, hence $A \subseteq \varphi^{-1}(\varphi(A))$. Also, we know that φ^{-1} is order-preserving, so that $\{1_H\} \subseteq \varphi(A)$ implies

$$\ker\varphi = \varphi^{-1}(\{1_H\}) \subseteq \varphi^{-1}(\varphi(A)).$$

We conclude that $\varphi^{-1}(\varphi(A))$ is an upper bound of A and $\ker\varphi$, hence it contains the least upper bound:

$$(A \vee \ker\varphi) \subseteq \varphi^{-1}(\varphi(A)).$$

Conversely, consider any element $g \in \varphi^{-1}(\varphi(A))$. By definition this means that $\varphi(g) \in \varphi(A)$, i.e., there exists $a \in A$ such that $\varphi(g) = \varphi(a)$. Since φ is a homomorphism this implies that $\varphi(a^{-1}g) = 1$ and hence $a^{-1}g \in \ker\varphi$. Finally, since $\ker\varphi \trianglelefteq G$ we know that $A\ker\varphi$ is a subgroup of G, hence

$$g = a(a^{-1}g) \in A\ker\varphi = A \vee \ker\varphi.$$

We conclude that $\varphi^{-1}(\varphi(A)) \subseteq (A \vee \ker\varphi)$.

Now we will show that $\varphi(\varphi^{-1}(B)) = (B \wedge \operatorname{im}\varphi)$. By general nonsense we know that $\varphi \circ \varphi^{-1}$ is a closure operator, hence $\varphi(\varphi^{-1}(B)) \subseteq B$. Also, we know that φ is order-preserving, so that $\varphi^{-1}(B) \subseteq G$ implies

$$\varphi(\varphi^{-1}(B)) \subseteq \varphi(G) = \operatorname{im}\varphi.$$

We conclude that $\varphi(\varphi^{-1}(B))$ is a lower bound of B and $\operatorname{im}\varphi$, hence it is contained in the greatest lower bound:

$$\varphi(\varphi^{-1}(B)) \subseteq (B \wedge \operatorname{im}\varphi).$$

Conversely, consider any element $h \in B \wedge \operatorname{im}\varphi = B \cap \operatorname{im}\varphi$. Since $h \in \operatorname{im}\varphi$, there exists $g \in G$ such that $\varphi(g) = h$. Then since $\varphi(g) = h \in B$ we have $g \in \varphi^{-1}(B)$. Finally, applying φ gives

$$h = \varphi(g) \in \varphi(\varphi^{-1}(B)).$$

We conclude that $(B \wedge \operatorname{im}\varphi) \subseteq \varphi(\varphi^{-1}(B))$. □

[Remark: It follows from this that the "Galois closed" subgroups of G are those containing the kernel and the "Galois closed" subgroups of H are those contained in the image.]

Problem 2. Terminal Objects. Consider an object X in a category $\mathcal{C}$. We say that X is an initial object if for all objects Y we have $|\mathrm{Hom}_{\mathcal{C}}(X,Y)| = 1$, and we say that X is a final object if for all objects Y we have $|\mathrm{Hom}_{\mathcal{C}}(Y,X)| = 1$.

(a) Prove that any two initial objects (resp. final objects) are isomorphic in $\mathcal{C}$.

(b) Determine the initial and final objects in the category of sets.

Proof. For part (a), let X and Y be objects in $\mathcal{C}$. If X and Y are either both initial or both final, then the sets

$$\mathrm{Hom}_{\mathcal{C}}(X,X), \quad \mathrm{Hom}_{\mathcal{C}}(X,Y), \quad \mathrm{Hom}_{\mathcal{C}}(Y,X), \quad \mathrm{Hom}_{\mathcal{C}}(Y,Y)$$

each contain exactly one arrow. Here is a picture of the four arrows:

$$\begin{tikzcd}
X \arrow[loop left, "\mathrm{id}_X"] \arrow[r, bend left, "\alpha"] & Y \arrow[l, bend left, "\beta"] \arrow[loop right, "\mathrm{id}_Y"]
\end{tikzcd}$$

Since $\beta \circ \alpha \in \mathrm{Hom}_{\mathcal{C}}(X,X)$ we conclude that $\beta \circ \alpha = \mathrm{id}_X$, and since $\alpha \circ \beta \in \mathrm{Hom}_{\mathcal{C}}(Y,Y)$ we conclude that $\alpha \circ \beta = \mathrm{id}_Y$. It follows that α and β are inverse isomorphisms.

For part (b), consider the category Set of sets and functions. If S and T are sets, recall that we can identify a function $f : S \to T$ with its graph $f \subseteq S \times T$ consisting of the pairs (s,t) such that $f(s) = t$. Note that isomorphisms in Set are just bijections. [Remark: Let $\mathcal{C}$ be a category. If we somehow replace each object in $\mathcal{C}$ by its isomorphism class we obtain a new category called the skeleton of $\mathcal{C}$. The skeleton of Set is called the category of cardinal numbers.]

First let $S = \emptyset$ and consider any other set T. The empty graph $\emptyset \subseteq S \times T$ defines a valid function $\emptyset : S \to T$, and this is the **only** valid function. We conclude that $\emptyset$ is an initial object in Set. The isomorphism class of $\emptyset$ is called $\mathbf{0}$.

Now let $T = \{t\}$ be a singleton and consider any other set S. The only valid function $f : S \to \{t\}$ is defined by $f(s) = t$ for all $s \in S$. Thus any singleton is a final object in the category Set. The isomorphism class of singletons is called $\mathbf{1}$.

□

Problem 3. Zero Objects and Zero Arrows. An object X in a category $\mathcal{C}$ is called a zero object if it is both initial and final. Suppose that the category $\mathcal{C}$ has a zero object $\mathbf{0}$ (which is unique up to isomorphism by Problem 1). Then between any two objects X and Y there is a unique zero arrow $0 : X \to Y$ defined by

$$\begin{tikzcd}
X \arrow[r] \arrow[rr, bend left, "0"] & \mathbf{0} \arrow[r] & Y
\end{tikzcd}$$

(a) Give an exmple of a category with no zero object.

(b) Describe the zero object and the zero arrows in the category of groups.

Proof. For part (a) we consider the category of sets. Recall from Problem 2(b) that the initial objects in Set are the sets with zero elements and the final objects in Set are the sets with one element. Since $0 \neq 1$ we conclude that this category has no zero objects.

For part (b) consider the category Grp of groups. Let $\mathbf{1} = \{1\}$ be a group with one element, and consider any other group G. There is a unique set function $\varphi : G \to \mathbf{1}$ sending every element to 1 and this function is necessarily a group homomorphism. Also, if $\varphi : \mathbf{1} \to G$ is a group homomorphism then it must send $1 \in \mathbf{1}$ to $1_G \in G$, and this property uniquely defines φ. We conclude that $\mathbf{1}$ is the zero object in Grp. Now consider any two groups G and H. The zero arrow (which we will call "1") is defined by

$$\begin{tikzcd}
G \arrow[r] \arrow[rr, bend left, "1"] & \mathbf{1} \arrow[r] & H
\end{tikzcd}$$

This map sends every element of G to the identity element $1_H \in H$. □

Problem 4. Universal Property of Kernels. Let $\mathcal{C}$ be a category with a zero object 0 and consider any arrow $\varphi : G \to G'$. Define a category $\mathcal{C}_\varphi$ whose objects are pairs (K, α) satisfying the commutative diagram

$$\begin{tikzcd}
K \arrow[r, "\alpha"'] \arrow[rr, bend left, "0"] & G \arrow[r, "\varphi"'] & G'
\end{tikzcd}$$

and whose morphisms $\sigma : (K_1, \alpha_1) \to (K_2, \alpha_2)$ are arrows $\sigma : K_1 \to K_2$ in $\mathcal{C}$ satisfying

$$\begin{tikzcd}
K_1 \arrow[d, "\sigma"'] \arrow[dr, "\alpha_1"] \arrow[drr, bend left, "0"] & & \\
& G \arrow[r, "\varphi"'] & G' \\
K_2 \arrow[ur, "\alpha_2"'] \arrow[urr, bend right, "0"'] & &
\end{tikzcd}$$

If this category has a **final object** (K, α) we will call it the kernel of $\varphi : G \to G'$. (Note that the kernel consists of both an object K and an arrow $\alpha : K \to G$.)

(a) Verify that $\mathcal{C}_\varphi$ is a category.

(b) Prove that every homomorphism in the category of groups has a kernel. [Hint: You already know what the kernel "should" be.]

Proof. For part (a) we must verify that morphisms in $\mathcal{C}_\varphi$ can be composed and that every object of $\mathcal{C}_\varphi$ has an identity morphism. First, suppose that we have objects (K_1, α_1), (K_2, α_2), and (K_3, α_3) with morphisms $\sigma : (K_1, \alpha_1) \to (K_2, \alpha_2)$ and $\tau : (K_2, \alpha_2) \to (K_3, \alpha_3)$. I claim that the arrow $\tau\sigma : K_1 \to K_3$ in $\mathcal{C}$ defines a morphism $\tau\sigma : (K_1, \alpha_1) \to (K_3, \alpha_3)$ in $\mathcal{C}_\varphi$. Indeed, consider the following diagrams:

$$\begin{tikzcd}
K_1 \arrow[d, "\sigma"] \arrow[dd, bend right, "\tau\sigma"'] \arrow[dr, "\alpha_1"] \arrow[drr, bend left, "0"] & & & & K_1 \arrow[dd, bend right, "\tau\sigma"'] \arrow[dr, "\alpha_1"] \arrow[drr, bend left, "0"] & & \\
K_2 \arrow[r, "\alpha_2"] \arrow[d, "\tau"] \arrow[rr, bend right, "0"] & G \arrow[r, "\varphi"] & G' & \Longrightarrow & & G \arrow[r, "\varphi"] & G' \\
K_3 \arrow[ur, "\alpha_3"'] \arrow[urr, bend right, "0"'] & & & & K_3 \arrow[ur, "\alpha_3"'] \arrow[urr, bend right, "0"'] & &
\end{tikzcd}$$

One can check that the diagram on the left commutes. [Only the arrow $\tau\sigma$ needs to be checked.] Since this diagram commutes, it **still** commutes after deleting the object K_2. The associativity of composition in $\mathcal{C}_\varphi$ is inherited from $\mathcal{C}$. Now let (K, α) be any object in $\mathcal{C}_\varphi$ and consider the identity arrow $\mathrm{id}_K : K \to K$ in $\mathcal{C}$. Note that the diagram

$$\begin{tikzcd}
K \arrow[d, "\mathrm{id}_K"'] \arrow[dr, "\alpha"] \arrow[drr, bend left, "0"] & & \\
& G \arrow[r, "\varphi"'] & G' \\
K \arrow[ur, "\alpha"'] \arrow[urr, bend right, "0"'] & &
\end{tikzcd}$$

commutes, so this defines a morphism $\mathrm{id}_{(K,\alpha)} : (K, \alpha) \to (K, \alpha)$ in $\mathcal{C}_\varphi$. Finally, consider any morphism $\sigma : (K_1, \alpha_1) \to (K_2, \alpha_2)$ in $\mathcal{C}_\varphi$ coming from $\sigma : K_1 \to K_2$ in $\mathcal{C}$. Since $\sigma \mathrm{id}_{K_1} = \sigma$ and $\mathrm{id}_{K_2}\sigma = \sigma$ in $\mathcal{C}$, it follows that $\sigma \mathrm{id}_{(K_1,\alpha_1)} = \sigma$ and $\mathrm{id}_{(K_2,\alpha_2)}\sigma = \sigma$ in $\mathcal{C}_\varphi$. We conclude that $\mathcal{C}_\varphi$ is a category.

For part (b), consider any group homomorphism $\varphi : G \to G'$. I claim that the arrow-theoretic kernel is given by the set-theoretic kernel $\ker \varphi$ and the inclusion homomorphism

$i : \ker\varphi \to G$. To prove this, first note that the definition of $\ker\varphi$ says exactly that the following diagram commutes:

$$\begin{tikzcd}
\ker\varphi \arrow[r, "i"'] \arrow[rr, bend left, "1"] & G \arrow[r, "\varphi"'] & G'
\end{tikzcd}$$

Thus $(\ker\varphi, i)$ is an object in Grp_φ. Now consider any object (K,α) in Grp_φ. We want to show that there exists a unique morphism $\bar{\alpha} : (K,\alpha) \to (\ker\varphi, i)$ such that the following diagram commutes:

$$\begin{tikzcd}
K \arrow[dr, "\alpha"] \arrow[drr, bend left, "1"] \arrow[dd, dashed, "\bar{\alpha}"'] & & \\
& G \arrow[r, "\varphi"'] & G' \\
\ker\varphi \arrow[ur, "i"'] \arrow[urr, bend right, "1"'] & &
\end{tikzcd}$$

To prove this, consider any element $k \in K$. If the map $\bar{\alpha}$ exists then commutativity implies $i(\bar{\alpha}(k)) = \alpha(k)$. On the other hand, since i is just the identity on $\ker\varphi$ we must have $i(\bar{\alpha}(k)) = \bar{\alpha}(k)$. Thus $\bar{\alpha}(k)$ is uniquely defined by $\bar{\alpha}(k) := \alpha(k)$ as long as $\alpha(k) \in \ker\varphi$. And we certainly **do** have $\alpha(k) \in \ker\varphi$ because commutativity of the diagram implies $\varphi(\alpha(k)) = 1 \in G'$. □

[Remark: The definition of categorical "cokernel" is given by reversing all the arrows in the definition of categorical kernel. Every group homomorphism $\varphi : G \to G'$ has a cokernel given by the projection $\pi : G' \to G'/N'$, where N' is the normal closure of the image $\operatorname{im}\varphi$ in G'.]

Problem 5. Universal Property of Products. Let $\mathcal{C}$ be a category. Given two objects A and B in $\mathcal{C}$ we define a new category $\mathcal{C}_{A,B}$ whose objects are triples (P,f,g) of the form

$$\begin{tikzcd}
& A \\
P \arrow[ur, "f"] \arrow[dr, "g"'] & \\
& B
\end{tikzcd}$$

and whose morphisms $\sigma : (P_1,f_1,g_1) \to (P_2,f_2,g_2)$ are arrows $\sigma : P_1 \to P_2$ in $\mathcal{C}$ satisfying

$$\begin{tikzcd}
& & A \\
P_1 \arrow[r, "\sigma"] \arrow[urr, bend left, "f_1"] \arrow[drr, bend right, "g_1"'] & P_2 \arrow[ur, "f_2"] \arrow[dr, "g_2"] & \\
& & B
\end{tikzcd}$$

If this category has a **final object** (P,f,g) we will call it the product of A and B. (Note that the product consists of both the object P and the arrows f,g.)

(a) Verify that $\mathcal{C}_{A,B}$ is a category.

(b) Prove that products exist in the category of groups. [Hint: You already know what the product "should" be.]

Proof. For part (a) we must verify that morphisms in $\mathcal{C}_{A,B}$ can be composed and that every object of $\mathcal{C}_{A,B}$ has an identity morphism. First, suppose that we have objects (P_1,f_1,g_1), (P_2,f_2,g_2), and (P_3,f_3,g_3) with morphisms $\sigma : (P_1,f_1,g_1) \to (P_2,f_2,g_2)$ and $\tau : (P_2,f_2,g_2) \to$

(P_3, f_3, g_3). I claim that the arrow $\tau\sigma : P_1 \to P_3$ in $\mathcal{C}$ defines a morphism $\tau\sigma : (P_1, f_1, g_1) \to (P_3, f_3, g_3)$ in $\mathcal{C}_{A,B}$. Indeed, consider the following diagrams:

$$\begin{tikzcd}
 & & & A & & & & A \\
P_1 \arrow[r, "\sigma"] \arrow[urrr, bend left, "f_1"] \arrow[drrr, bend right, "g_1"'] \arrow[rr, bend right, "\tau\sigma"'] & P_2 \arrow[r, "\tau"] \arrow[urr, bend left, "f_2"] \arrow[drr, bend right, "g_2"'] & P_3 \arrow[ur, "f_3"] \arrow[dr, "g_3"'] & & \Longrightarrow & P_1 \arrow[urr, bend left, "f_1"] \arrow[drr, bend right, "g_1"'] \arrow[r, bend right, "\tau\sigma"'] & P_3 \arrow[ur, "f_3"] \arrow[dr, "g_3"'] & \\
 & & & B & & & & B
\end{tikzcd}$$

One can check that the diagram on the left commutes. [Only the arrow $\tau\sigma$ needs to be checked.] Since this diagram commutes, it **still** commutes after deleting the object P_2. The associativity of composition in $\mathcal{C}_{A,B}$ is inherited from $\mathcal{C}$. Now let (P, f, g) be any object in $\mathcal{C}_{A,B}$ and consider the identity arrow $\mathrm{id}_P : P \to P$ in $\mathcal{C}$. Note that the diagram

$$\begin{tikzcd}
 & & A \\
P \arrow[r, "\mathrm{id}_P"] \arrow[urr, bend left, "f"] \arrow[drr, bend right, "g"'] & P \arrow[ur, "f"] \arrow[dr, "g"'] & \\
 & & B
\end{tikzcd}$$

commutes, so this defines a morphism $\mathrm{id}_{(P,f,g)} : (P, f, g) \to (P, f, g)$ in $\mathcal{C}_{A,B}$. Finally, consider any morphism $\sigma : (P_1, f_1, g_1) \to (P_2, f_2, g_2)$ in $\mathcal{C}_{A,B}$ coming from $\sigma : P_1 \to P_2$ in $\mathcal{C}$. Since $\sigma \mathrm{id}_{P_1} = \sigma$ and $\mathrm{id}_{P_2}\sigma = \sigma$ in $\mathcal{C}$, it follows that $\sigma\mathrm{id}_{(P_1,f_1,g_1)} = \sigma$ and $\mathrm{id}_{(P_2,f_2,g_2)}\sigma = \sigma$ in $\mathcal{C}_{A,B}$. We conclude that $\mathcal{C}_{A,B}$ is a category.

For part (b), let A and B be groups and consider the direct prouct group $A \times B$ defined by

$$(a_1, b_1) \bullet (a_2, b_2) := (a_1 a_2, b_1 b_2).$$

Let $\pi_A : A \times B \to A$ and $\pi_B : A \times B \to B$ be the projection homomorphisms defined by $\pi_A(a, b) = a$ and $\pi_B(a, b) = b$. I claim that the triple $(A \times B, \pi_A, \pi_B)$ is a final object in the category $\mathsf{Grp}_{A,B}$. To prove this, consider any object (P, f, g) of $\mathsf{Grp}_{A,B}$. We want to show that there exists a unique morphism $f \times g : (P, f, g) \to (A \times B, \pi_A, \pi_B)$ such that the following diagram commutes:

$$\begin{tikzcd}
 & & A \\
P \arrow[r, dashed, "f \times g"] \arrow[urr, bend left, "f"] \arrow[drr, bend right, "g"'] & A \times B \arrow[ur, "\pi_A"] \arrow[dr, "\pi_B"'] & \\
 & & B
\end{tikzcd}$$

To prove this, consider any element $p \in P$. If the map $f \times g$ exists then we must have $(f \times g)(p) = (p_A, p_B)$ for some elements $p_A \in A$ and $p_B \in B$ such that $f(p) = \pi_A(p_A, p_B) = p_A$ and $g(p) = \pi_B(p_A, p_B) = p_B$. Such elements p_A and p_B certainly **do** exist. □

[Remark: The definition of categorical "coproduct" is given by reversing all the arrows in the definition of categorical product. Coproducts also exist in the category of groups. The coproduct of groups A and B is called their "free product" $A * B$.]

Problem 6. Semi-Direct Products. Consider two groups N and G and a group homomorphism $\varphi : G \to \mathrm{Aut}_{\mathsf{Grp}}(N)$. We use φ to define a binary operation on the Cartesian product set $N \times G$ as follows:

$$(n_1, g_1) \bullet (n_2, g_2) := (n_1\varphi_{g_1}(n_2), g_1g_2).$$

Let $N \rtimes_\varphi G$ denote the triple $(N \times G, \bullet, (1_N, 1_G))$. We call this the semi-direct product of N and G with respect to φ.

(a) Prove that $N \rtimes_\varphi G$ is a group.

(b) Identify N and G with subgroups of $N \rtimes_\varphi G$ via the maps $n \mapsto (n, 1_G)$ for $n \in N$ and and $g \mapsto (1_N, g)$ for $g \in G$. Prove that

$$N \cap G = 1, \quad N \trianglelefteq N \rtimes_\varphi G, \quad \text{and} \quad NG = N \rtimes_\varphi G.$$

(c) Finally, prove that for all $n \in N$ and $g \in G$ we have $\varphi_g(n) = gng^{-1}$.

Proof. For part (a) we must show that the operation $\bullet$ is associative, with an identity element and inverses. First note that for all $n \in N$ and $g \in G$ we have $\varphi_g(1_N) = 1_N$ (since φ_g is a homomorphism) and $\varphi_{1_G}(n) = n$ (since φ is a homomorphism). Then for any element $(n, g) \in N \times G$ we have

$$(1_N, 1_G) \bullet (n, g) = (1_N\varphi_{1_G}(n), 1_N g) = (n, g) = (n\varphi_g(1_N), g1_G) = (n, g) \bullet (1_N, 1_G),$$

hence $(1_N, 1_G) \in N \times G$ is an identity element. Next observe that the element $(n, g) \in N \times G$ has inverse $(\varphi_{g^{-1}}(n^{-1}), g^{-1})$ because

$$\begin{aligned}(n, g) \bullet (\varphi_{g^{-1}}(n^{-1}), g^{-1}) &= (n\varphi_g(\varphi_{g^{-1}}(n^{-1})), gg^{-1}) \\ &= (n\varphi_{gg^{-1}}(n^{-1}), 1_G) \\ &= (n\varphi_{1_G}(n^{-1}), 1_G) \\ &= (nn^{-1}, 1_G) \\ &= (1_N, 1_G).\end{aligned}$$

and

$$\begin{aligned}(\varphi_{g^{-1}}(n^{-1}), g^{-1}) \bullet (n, g) &= (\varphi_{g^{-1}}(n^{-1})\varphi_{g^{-1}}(n), g^{-1}g) \\ &= (\varphi_{g^{-1}}(n^{-1}n), 1_G) \\ &= (\varphi_{g^{-1}}(1_N), 1_G) \\ &= (1_N, 1_G).\end{aligned}$$

Finally, observe that for all $n_1, n_2, n_3 \in N$ and $g_1, g_2, g_3 \in G$ we have

$$\begin{aligned}[(n_1, g_1) \bullet (n_2, g_2)] \bullet (n_3, g_3) &= (n_1\varphi_{g_1}(n_2), g_1g_2) \bullet (n_3, g_3) \\ &= (n_1\varphi_{g_1}(n_2)\varphi_{g_1g_2}(n_3), g_1g_2g_3) \\ &= (n_1\varphi_{g_1}(n_2)\varphi_{g_1}(\varphi_{g_2}(n_3)), g_1g_2g_3) \\ &= (n_1\varphi_{g_1}(n_2\varphi_{g_2}(n_3)), g_1g_2g_3) \\ &= (n_1, g_1) \bullet (n_2\varphi_{g_2}(n_3), g_2g_3) \\ &= (n_1, g_1) \bullet [(n_2, g_2) \bullet (n_3, g_3)].\end{aligned}$$

We conclude that $(N \times H, \bullet, (1_N, 1_G))$ is a group.

For part (b) we will identify N and G with subgroups of $N \rtimes_\varphi G$ via the injective homomorphisms $n \mapsto (n, 1_G)$ and $g \mapsto (1_N, g)$. Under these identifications we will show that the external semi-direct product agrees with the internal semi-direct product, i.e., $N \rtimes_\varphi G = N \rtimes G$. First note that $N \rtimes_\varphi G = NG$ because for all $(n,g) \in N \times G$ we have

$$n \bullet g = (n, 1_G) \bullet (1_N, g) = (n\varphi_{1_G}(1_N), 1_G g) = (n1_N, g) = (n, g).$$

Next note that $N \cap G = 1$ because the only element simultaneously of the form $(n, 1_G)$ and $(1_N, g)$ is $(1_N, 1_G)$. Finally, note that N is normal in $N \rtimes_\varphi G$ since for all $(a, 1_G) \in N$ and $(n,g) \in N \times G$ we have

$$\begin{aligned}
(n,g) \bullet (a, 1_G) \bullet (n,g)^{-1} &= (n,g) \bullet (a, 1_G) \bullet (\varphi_{g^{-1}}(n^{-1}), g^{-1}) \\
&= (n\varphi_g(a), g1_G) \bullet (\varphi_{g^{-1}}(n^{-1}), g^{-1}) \\
&= (n\varphi_g(a), g) \bullet (\varphi_{g^{-1}}(n^{-1}), g^{-1}) \\
&= (n\varphi_g(a)\varphi_g(\varphi_{g^{-1}}(n^{-1})), gg^{-1}) \\
&= (n\varphi_g(a)\varphi_{gg^{-1}}(n^{-1}), 1_G) \\
&= (n\varphi_g(a)\varphi_{1_G}(n^{-1}), 1_G) \\
&= (n\varphi_g(a)n^{-1}, 1_G) \in N.
\end{aligned}$$

For part (c) we will verify that the conjugation action of the subgroup G on the normal subgroup N agrees with the homomorphism $\varphi : G \to \mathrm{Aut}_{\mathsf{Grp}}(H)$ we used to define the semi-direct product. Indeed, for all $n \in N$ and $g \in G$ the previous computation implies that

$$\begin{aligned}
g \bullet n \bullet g^{-1} &= (1_N, g) \bullet (n, 1_G) \bullet (1_N, g)^{-1} \\
&= (1_N\varphi_g(n)1_N^{-1}, 1_G) \\
&= (\varphi_g(n), 1_G) \\
&= \varphi_g(n).
\end{aligned}$$

□

Problem 7. Dihedral Groups. A dihedral group is the semi-direct product of a cyclic group $\langle R \rangle$ of arbitrary order with a cyclic group $\langle F \rangle$ of order 2, via the homomorphism $\varphi : \langle F \rangle \to \mathrm{Aut}_{\mathsf{Grp}}(\langle R \rangle)$ defined by $\varphi_F(R) = R^{-1}$.

Now let G be a group containing two involutions $a, b \in G$ (i.e., $a, b \neq 1$ and $a^2, b^2 = 1$). Prove that the subgroup $\langle a, b \rangle \subseteq G$ generated by a and b is isomorphic to a dihedral group. [Hint: Let $F = a$ and $R = ab$.]

Proof. First note that $\langle a, b \rangle$ contains the set $\{a, ab\}$, hence it must contain the group $\langle a, ab \rangle = \langle \{a, ab\} \rangle$. Conversely, note that $b = a(ab) \in \langle a, ab \rangle$ so that $\langle a, ab \rangle$ contains the set $\{a, b\}$, and hence the group $\langle a, b \rangle = \langle \{a, b\} \rangle$. We conclude that $\langle a, b \rangle = \langle a, ab \rangle$.

To prove that $\langle a, ab \rangle$ is dihedral we must show: (1) $\langle ab \rangle \trianglelefteq \langle a, ab \rangle$, with a acting on $\langle ab \rangle$ by inversion, (2) $\langle a \rangle \cap \langle ab \rangle = 1$, and (3) $\langle a, ab \rangle = \langle a \rangle \langle ab \rangle$. Throughout we will use the fact that $a^{-1} = a$ and $b^{-1} = b$.

For (1), first note that $(ab)(ba) = ab^2a = a1a = a^2 = 1 = b^2 = b1b = ba^2b = (ba)(ab)$, hence $(ab)^{-1} = ba$. I claim that $a(ab)^n a = (ab)^{-n}$ for all $n \in \mathbb{Z}$. Indeed, we have $a(ab)^0 a = a1a = a^2 = 1 = (ab)^{-0}$. Now suppose for induction that we have $a(ab)^n a = (ab)^{-n}$ (hence also $(ab)^n = a(ab)^{-n}a)$ for some $n \geq 1$. Then we have

$$\begin{aligned} a(ab)^{n+1}a &= a(ab)^n(ab)a \\ &= [a(ab)^n a](ba) \\ &= (ab)^{-n}(ab)^{-1} \\ &= (ab)^{-(n+1)} \end{aligned}$$

(hence also $(ab)^{n+1} = a(ab)^{-(n+1)}a)$. It follows that $\langle ab \rangle \trianglelefteq \langle a, ab \rangle$, and moreover that the element a acts on $\langle ab \rangle$ by inversion.

For (2), we want to show that $a \neq (ab)^n$ for all $n \in \mathbb{Z}$. First note that we have $a \neq (ab)^0$ (i.e., $a \neq 1$) and $a \neq (ab)^1$ (i.e., $b \neq 1$). Now assume for induction that $a = (ab)^{n+2}$. In this case we have

$$\begin{aligned} a &= (ab)(ab)^{n+1} \\ 1 &= b(ab)^{n+1} \\ 1 &= (ba)^{n+1}b \\ b &= (ba)^{n+1} \\ b &= (ba)(ba)^n \\ 1 &= a(ba)^n \\ 1 &= (ab)^n a \\ a &= (ab)^n. \end{aligned}$$

We have shown that $a \neq (ab)^n \Rightarrow a \neq (ab)^{n+2}$. Combined with the initial conditions this proves that $a \neq (ab)^n$ for all integers $n \geq 0$. Then since $a = a^{-1}$ we conclude that $a \neq (ab)^n$ for all integers $n < 0$.

For (3), note that every element of the group $\langle a, ab \rangle = \langle a, b \rangle$ has the form

$$a, ab, aba, abab, \ldots, \qquad \text{or} \qquad b, ba, bab, baba, \ldots.$$

In other words, every element has the form $a(ba)^n$, $(ab)^n$, $(ba)^n b$, or $(ba)^n$ for some integer $n \geq 0$. Note that

$$\begin{aligned} a(ba)^n &= a(ab)^{-n} && \in \langle a \rangle \langle ab \rangle, \\ (ab)^n &= 1(ab)^n && \in \langle a \rangle \langle ab \rangle, \\ (ba)^n &= 1(ab)^{-n} && \in \langle a \rangle \langle ab \rangle, \\ (ba)^n b &= aa(ba)^n b = a(ab)^{n+1} && \in \langle a \rangle \langle ab \rangle. \end{aligned}$$

We conclude that $\langle a, ab \rangle \subseteq \langle a \rangle \langle ab \rangle$, and hence $\langle a, ab \rangle = \langle a \rangle \langle ab \rangle$.

The fact that $\langle a, b \rangle$ is isomorphic to $\langle F \rangle \ltimes_\varphi \langle R \rangle$ now follows from Problem 6. I won't spell out the details, and I don't mind if you don't either. □