Math 761 **Fall 2015**
Homework 3 **Drew Armstrong**

Problem 1. Modularity. Let $(\mathscr{L}, \leq, \wedge, \vee, 0, 1)$ be a lattice. For all $x, y \in \mathscr{L}$ we define the closed interval $[x, y] := \{z \in \mathscr{L} : x \leq z \leq y\}$.

(a) Prove that for all $a, b \in \mathscr{L}$ we have a Galois connection

$$a \vee (-) : [0, b] \rightleftarrows [a, 1] : (-) \wedge b.$$

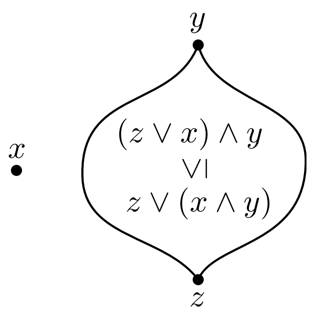
In other words, show that for all $x \in [0, b]$ and $y \in [a, 1]$ we have

$$x \leq (y \wedge b) \iff (a \vee x) \leq y.$$

(b) Given elements $x, y, z \in \mathscr{L}$ with $z \leq y$, there are two possible way to map the element x into the interval $[z, y]$: by meeting with y and then joining with z, or by joining with z and then meeting with y. Prove that these two images are related by

$$z \vee (x \wedge y) \leq (z \vee x) \wedge y \tag{1}$$

as in the following picture:



We will say that $(a, b) \in \mathscr{L}^2$ is a modular pair if for all $x \leq b$ and $a \leq y$ the inequality (1) becomes an **equality**; that is, if we have

$$x \vee (a \wedge b) = (x \vee a) \wedge b, \quad \text{and} \tag{2}$$

$$a \vee (b \wedge y) = (a \vee b) \wedge y. \tag{3}$$

We will say that $a \in \mathscr{L}$ is a modular element if (a, b) is a modular pair for all $b \in \mathscr{L}$.

(c) If (a, b) is a modular pair, prove that the Galois connection from part (a) restricts to an isomorphism of lattices

$$[a \wedge b, b] \approx [a, a \vee b].$$

Proof. For part (a), consider any $x \leq b$ and $y \geq a$. If $x \leq (y \wedge b)$ then since $(y \wedge b) \leq y$ we have $x \leq y$. Now y is an upper bound of a and x, so it must be greater than the least upper bound: $(a \vee x) \leq y$. Conversely, if $(a \vee x) \leq y$ then since $x \leq (a \vee x)$ we have $x \leq y$. Now x is a lower bound of y and b, so it must be less than the greatest lower bound: $x \leq (y \wedge b)$. We conclude that the pair of maps $a \vee (-) : [0, b] \rightleftarrows [a, 1] : (-) \wedge b$ is a (covariant) Galois connection, hence all of the (suitably-modified) theorems from HW1 apply.

For part (b), suppose that we have $x, y, z \in \mathscr{L}$ with $z \leq y$, as in the diagram above. First note that $(x \wedge y) \leq y$ and $(x \wedge y) \leq x \leq (z \vee x)$. Since $x \wedge y$ is a lower bound of $z \vee x$ and y, it is less than the greatest lower bound:

$$(x \wedge y) \leq (z \vee x) \wedge y. \tag{4}$$

Similarly, since $z \leq y$ and $z \leq (z \vee x)$ we have

$$z \leq (z \vee x) \wedge y. \tag{5}$$

Finally, (4) and (5) say that $(z \vee x) \wedge y$ is an upper bound of z and $x \vee y$, hence it is greater than the least upper bound:

$$z \vee (x \wedge y) \leq (z \vee x) \wedge y.$$

For part (c), first recall from HW1 that a Galois connection restricts to a poset isomorphism between closed elements. In particular, the Galois connection from part (a) restricts to an isomorphism

$$a \vee (-) : [a,1]^* \rightleftarrows [0,b]^* : (-) \wedge b.$$

where $[a,1]^* \subseteq [0,b]$ is the subposet of elements $x \in [0,b]$ such that $x = (a \vee x) \wedge b$ and $[0,b]^* \subseteq [a,1]$ is the subposet of elements $y \in [a,1]$ such that $y = a \vee (y \wedge b)$. Note that $[a,1]^* \subseteq [a \wedge b, b]$ and $[0,b]^* \subseteq [a, a \vee b]$. If (a,b) is a modular pair, I claim that these two inclusions are equalities. For the first equality, consider any $x \in [a \wedge b, b]$. Since (a,b) is a modular pair and $x \leq b$, equation (2) holds. Then since $(a \wedge b) \leq x$ we have

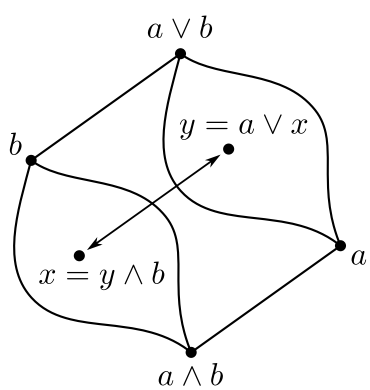
$$x = x \vee (a \wedge b) = (x \vee a) \wedge b = (a \vee x) \wedge b.$$

For the second equality, consider any $y \in [a, a \vee b]$. Since (a,b) is a modular pair and $a \leq y$, equation (3) holds. Then since $y \leq (a \vee b)$ we have

$$y = (a \vee b) \wedge y = a \vee (b \wedge y) = a \vee (y \wedge b).$$

$\square$

[Remark: In summary, let $\mathscr{L}$ be a lattice and consider two elements $a, b \in \mathscr{L}$. If a is a modular element (more generally, if (a,b) is a modular pair) then we obtain an isomorphism as in the following diagram:



The concept of a lattice (under the name "dual group") was invented by Dedekind around 1900. He called a lattice in which every element is modular a "dual group of module-type" because lattices of submodules satisfy this property. The concept of a modular **element** was isolated by Kurosh in 1940.]

Problem 2. Normal $\Rightarrow$ Modular. Let G be a group and consider its lattice $\mathscr{L}(G)$ of subgroups. Let $H, N \in \mathscr{L}(G)$ with $N \trianglelefteq G$.

(a) Prove that N is a modular element of the lattice $\mathscr{L}(G)$ and conclude from Problem 1 that we have an isomorphism of lattices

$$[H \wedge N, H] \approx [N, H \vee N].$$

(b) Prove that the lattice isomorphism from part (a) lifts to an isomorphism of groups

$$\frac{H}{H \wedge N} \approx \frac{H \vee N}{N}.$$

[Hint: Since $N \trianglelefteq G$ we have $H \vee N = HN$ and $N \trianglelefteq HN$. Consider the function $\varphi : H \to HN/N$ defined by $\varphi(h) = (h1)N$.]

Proof. For part (a) we will prove that (N, H) is a modular pair. Since H is arbitrary, this will prove that N is a modular element. So consider any other subgroup $K \in \mathscr{L}(G)$. We want to prove that

$$K \subseteq H \Longrightarrow K \vee (N \wedge H) = (K \vee N) \wedge H, \quad \text{and} \tag{6}$$

$$N \subseteq K \Longrightarrow N \vee (H \wedge K) = (N \vee H) \wedge K. \tag{7}$$

To show (6), assume that $K \subseteq H$. We already know from Problem 1(b) that

$$K \vee (N \wedge H) \subseteq (K \vee N) \wedge H.$$

To show the other direction first note that K normalizes $N \cap H$. Indeed, given $k \in K$ and $h \in N \cap H$ we have $khk^{-1} \in N$ since $N \trianglelefteq G$ and $khk^{-1} \in H$ since $K \subseteq H$, hence $khk^{-1} \in N \cap H$. This implies that $K \vee (N \cap H) = K(N \cap H)$ and since K clearly normalizes N we also have $K \vee N = KN$. Thus we want to show that

$$(KN) \cap H \subseteq K(N \cap H).$$

So consider any $k \in K$ and $n \in N$ such that $kn \in H$. Since $K \subseteq H$ we have $n = k^{-1}(kn) \in H$, and it follows that $kn \in K(N \cap H)$ as desired.

To show (7), assume that $N \subseteq K$. We already know from Problem 1(b) that

$$N \vee (H \wedge K) \subseteq (N \vee H) \wedge K.$$

To show the other direction first note that since $N \trianglelefteq G$ we have $N \vee (H \wedge K) = N(H \cap K)$ and $(N \vee H) \wedge K = (NH) \cap K$. Thus we want to show that

$$(NH) \cap K \subseteq N(H \cap K).$$

So consider any $n \in N$ and $h \in H$ such that $nh \in K$. Since $N \subseteq K$ we have $h = n^{-1}(nh) \in K$, and it follows that $nh \in N(H \cap K)$ as desired.

For part (b), first note that since $N \trianglelefteq G$ we have $H \vee N = HN$ and $N \trianglelefteq HN$. Now define a function $\varphi : H \to HN/N$ by $\varphi(h) = hN$ and note that for all $h_1, h_2 \in H$ we have

$$\varphi(h_1)\varphi(h_2) = (h_1N)(h_2N) = (h_1h_2)N = \varphi(h_1h_2),$$

hence φ is a homomorphism. The homomorphism is surjective since for all $hn \in HN$ we have $\varphi(h) = hN = h(nN) = (hn)N$. Finally, since the kernel of φ is $H \cap N$, the First Isomorphism Theorem says that

$$\frac{H}{H \wedge N} = \frac{H}{H \cap N} = \frac{H}{\ker \varphi} \approx \operatorname{im} \varphi = \frac{HN}{N} = \frac{H \vee N}{N}.$$

□

[Remark: Let $N, H, K \in \mathscr{L}(G)$ with $N \trianglelefteq G$. Apart from the conditions (6) and (7), there is a third reasonable condition that we might expect:

$$K \subseteq N \Longrightarrow K \vee (H \wedge N) = (K \vee H) \wedge N.$$

But this third condition is **not** true, which motivates the strange-looking definition of "modular element". It would be a beautiful result if every modular element of $\mathscr{L}(G)$ were normal. Sadly, this is also not true.]

Problem 3. Modular $\not\Rightarrow$ Normal. Consider the dihedral group D_6 and the cyclic group $\mathbb{Z}/3\mathbb{Z}$. Prove that we have an isomorphism of lattices

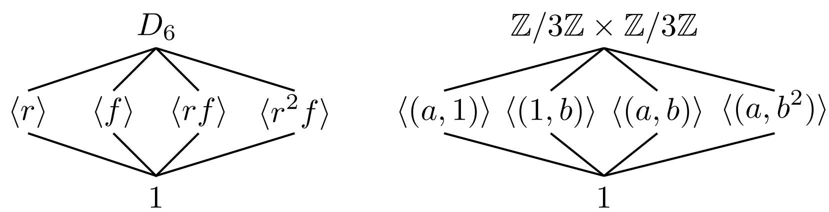
$$\mathscr{L}(D_6) \approx \mathscr{L}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}).$$

Conclude that a modular element of the subgroup lattice is not necessarily normal.

Proof. Let $D_6 = \langle r, f : r^3 = f^2 = 1, frf = r^2 \rangle = \{1, r, r^2, f, rf, r^2 f\}$. Note that D_6 has subgroups $\langle f \rangle$, $\langle rf \rangle$, and $\langle r^2 f \rangle$ of order 2. Any nontrivial subgroup containing one of the elements $f, rf, r^2 f$ would contain one of these subgroups, hence it would have order strictly dividing 6 and strictly divisible by 2. Contradiction. Any other nontrivial subgroup is contained $\{1, r, r^2\}$, hence $\langle r \rangle$ is the only possibility.

Let $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \langle a \rangle \times \langle b \rangle$. The only possible size of a nontrivial subgroup is 3 and any such subgroup must be cyclic. We easily see that there are four possibilities: $\langle (a,1) \rangle$, $\langle (1,b) \rangle$, $\langle (a,b) \rangle$, and $\langle (a,b^2) \rangle$.

The subgroup lattices are shown below:



Note that any bijection matching the four nontrivial subgroups will be an isomorphism of lattices. Since $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is an abelian group all of its subgroups are normal, so by Problem 2(a) every element of the lattice $\mathscr{L}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$ is modular. By the isomorphism this implies that every element of the lattice $\mathscr{L}(D_6)$ is modular. But the three subgroups $\langle f \rangle$, $\langle rf \rangle$, and $\langle r^2 f \rangle$ are **non-normal** in D_6. Too bad. This problem also demonstrates that the subgroup lattice can't tell if a group is abelian. $\square$

[Remark: This problem shows that the subgroup lattice is a fairly weak invariant of groups. There are still plenty of applications (for example, the property of "solvability" is purely lattice-theoretic) but in general the "internal" lattice structure must be supplemented by the "external" category structure. Compare the lattice-theoretic proof of 2(a) with the category-theoretic proof of 2(b).]

Problem 4. A Zappa–Szép Product. Let $H, K \subseteq G$ be subgroups. We say that G is a Zappa–Szép product of H and K (and we write $G = H \bowtie K$) if $H \wedge K = 1$, $H \vee K = G$, and **neither** of H or K is normal in G.

(a) Let $H, K \subseteq G$ be finite subgroups, at least one of which is normal in G. Prove that

$$|H| \cdot |K| = |HK| \cdot |H \cap K|.$$

[Hint: Use Problem 2(b).]

(b) Prove that the result of part (a) holds even in the case when both of H and K are non-normal. [Hint: Let H act by left multiplcation on the set of left cosets G/K. Show that HK is the disjoint union of cosets in the orbit of $K \in G/K$. How many such cosets are there?]

(c) Consider a cycle $c = (i_1 i_2 \cdots i_k) \in S_n$ and a permutation $\pi \in S_n$. Prove that

$$\pi c \pi^{-1} = (\pi(i_1)\pi(i_2) \cdots \pi(i_k)).$$

Use this fact to describe the conjugacy classes of S_n.

(d) Let $G = S_4$, $H = \langle (1234), (12)(34) \rangle$, and $K = \langle (123) \rangle$. Prove that $G = H \bowtie K$. [Hint: Show that $H \approx D_8$ and $K \approx \mathbb{Z}/3\mathbb{Z}$. Now use parts (b) and (c).]

Proof. For part (a), let $H, K \subseteq G$ be finite subgroups and assume without loss of generality that K is normal in G. Then Problem 2(b) tells us that the group $H/(H \cap K)$ is isomorphic to $(HK)/K$, and then Lagrange's Theorem implies

$$|H|/|H \cap K| = |H/(H \cap K)| = |(HK)/K| = |HK|/|K|.$$

[Remark: I never proved Lagrange's Theorem in class, so here's a proof. Let G be a finite group with $N \trianglelefteq G$. Note that there is a bijection between any two cosets $aN \to bN$ given by $g \mapsto ba^{-1}g$, thus every coset has size $|N|$. Since G is a disjoint union of cosets we conclude that $|G| = |G/N| \cdot |N|$.]

For part (b), let $H, K \subseteq G$ be finite subgroups, both possibly non-normal. For every element $h \in H$ we define a function $\varphi_h : G/K \to G/K$ by $\varphi_h(gK) := (hg)K$. Note that this function is invertible with inverse $\varphi_h^{-1} = \varphi_{h^{-1}}$. Now consider the set $\mathrm{Orb}_H(K) := \{\varphi_h(K) : h \in H\} = \{hK : h \in H\}$ and the set $\mathrm{Stab}_H(K) = \{h \in H : hK = K\} = \{h \in H : k \in K\} = H \cap K$. Note that the set HK is the disjoint union of the elements of $\mathrm{Orb}_H(K)$. Since every element of $\mathrm{Orb}_H(K)$ has size K this implies that $|HK| = |K| \cdot |\mathrm{Orb}_H(K)|$. Finally, the Orbit-Stabilizer Theorem says $|\mathrm{Orb}_H(K)| = |H|/|\mathrm{Stab}_H(K)| = |H|/|H \cap K|$, and hence

$$|HK| = |K| \cdot |\mathrm{Orb}_H(K)| = |K| \cdot |H|/|H \cap K|.$$

[Remark: I also didn't prove the Orbit-Stabilizer Theorem in class. I'll do this when we discuss the category of G-sets.]

For part (c), consider a cycle $c = (i_1 i_2 \cdots i_k) \in S_n$ and an arbitrary permutation $\pi \in S_n$. For all $j \in \{1, 2, \ldots, k\}$, the permutation $\pi c \pi^{-1}$ acts on the symbol $\pi(i_j)$ by

$$\pi(i_j) \xrightarrow{\pi^{-1}} i_j \xrightarrow{c} i_{(j+1 \bmod k)} \xrightarrow{\pi} \pi(i_{(j+1 \bmod k)}).$$

Also, for $m \notin \{i_1, \ldots, i_k\}$ we have $\pi(m) \notin \{\pi(i_1), \ldots, \pi(i_k)\}$, and hence $\pi c \pi^{-1}(\pi(m)) = \pi(c(m)) = \pi(m)$. This proves the result. As discussed in class, this implies that permutations are conjugate if and only if they have the same numer of cycles of each size.

For part (d), let $G = S_4$, $H = \langle (1234), (12)(34) \rangle$, and $K = \langle (123) \rangle$. Let $r = (1234)$ and $f = (12)(34)$. Since f and $rf = (13)$ are involutions we conclude from HW2 Problem 7 that $H \approx D_8$, and hence $|H| = 8$. Note that r and r^{-1} are the only elements of H with order 4. But we know from part (c) that (1234) is conjugate in G to all six 4-cycles, which implies that H is not normal. Next observe that $|K| = 3$ since (123) has order 3. But part (c) implies that (123) is conjugate to all eight 3-cycles in G, hence K is not normal. Finally, since $|H| = 8$ we know that H has no elements of order 3, hence $H \cap K = 1$. It follow from part (b) that

$$|H \vee K| \geq |HK| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{8 \cdot 3}{1} = 24 = |G|,$$

and hence $H \vee K = G$. □

Problem 5. Right-Split Exact Sequences. A short exact sequence in the category of groups is a sequence of groups and homomorphisms of the form

$$\mathbf{1} \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow \mathbf{1}$$

that satisfies $\ker \alpha = 1$, $\operatorname{im} \alpha = \ker \beta$, and $\operatorname{im} \beta = H$. Given such a sequence, prove that the following two conditions are equivalent.

(1) There exists a group homomorphism $s : H \to G$ such that $\beta \circ s = \mathrm{id}_H$. [This s is called a section of β.] In this case we say that the short exact sequence is right-split.

(2) There exists a homomorphism $\varphi : H \to \mathrm{Aut}(N)$ and an isomorphism $\gamma : N \rtimes_\varphi H \to G$ such that the following diagram commutes:

$$\begin{tikzcd}
\mathbf{1} \arrow[r] & N \arrow[r] \arrow[d, "\mathrm{id}_N"] & N \rtimes_\varphi H \arrow[r] \arrow[d, "\gamma"] & H \arrow[r] \arrow[d, "\mathrm{id}_H"] & \mathbf{1} \\
\mathbf{1} \arrow[r] & N \arrow[r, "\alpha"] & G \arrow[r, "\beta"] & H \arrow[r] & \mathbf{1}
\end{tikzcd}$$

The maps in the top row are the obvious ones.

[Hint: To prove that (1) $\Rightarrow$ (2), consider any $h \in H$ and $n \in N$. Prove that there exists a unique $n' \in N$ such that $s(h)\alpha(n)s(h^{-1}) = \alpha(n')$. Call it $\varphi_h(n) := n'$. Show that this defines a group homomorphism $\varphi : H \to \mathrm{Aut}(N)$. Now define a function $\gamma : N \rtimes_\varphi H \to G$ by $\gamma(n,h) := \alpha(n)s(h)$ and show that this is an isomorphism. To prove that (2) $\Rightarrow$ (1), define a function $s : H \to G$ by $s(h) := \gamma(1,h)$ and show that it has the desired properties.]

Proof. To prove that (1) $\Rightarrow$ (2), assume that we have a homomorphism $s : H \to G$ such that $\beta(s(h)) = h$ for all $h \in H$. Now consider any $h \in H$ and $n \in N$ and define the element $g := s(h)\alpha(n)s(h^{-1}) \in G$. Since $\mathrm{im}\,\alpha \subseteq \ker\beta$ we have

$$\beta(g) = \beta(s(h))\beta(\alpha(n))\beta(s(h^{-1})) = h1_Hh^{-1} = 1_H,$$

and hence $g \in \ker\beta$. Then since $\ker\beta \subseteq \mathrm{im}\,\alpha$, there exists $n' \in N$ such that $g = \alpha(n')$, and since α is injective this n' is unique. Thus for all $h \in H$ we have a function $\varphi_h : N \to N$, where $\varphi_h(n) \in N$ is the unique solution to the equation

$$s(h)\alpha(n)s(h^{-1}) = \alpha(\varphi_h(n)). \tag{8}$$

I claim that this $\varphi_h : N \to N$ is in fact a group automorphism. To see that it is a homomorphism, consider $n_1, n_2 \in N$ and note that

$$\begin{aligned}
\alpha(\varphi_h(n_1)\varphi_h(n_1)) &= \alpha(\varphi_h(n_1))\alpha(\varphi_h(n_2)) \\
&= s(h)\alpha(n_1)s(h^{-1})s(h)\alpha(n_2)s(h^{-1}) \\
&= s(h)\alpha(n_1)s(h^{-1}h)\alpha(n_2)s(h^{-1}) \\
&= s(h)\alpha(n_1)\alpha(n_2)s(h^{-1}) \\
&= s(h)\alpha(n_1n_2)s(h^{-1}),
\end{aligned}$$

hence $\varphi_h(n_1n_2) = \varphi_h(n_1)\varphi_h(n_2)$ by equation (8). To show that φ_h is bijective, note that for all $h_1, h_2 \in H$ and $n \in N$ we have

$$\begin{aligned}
\alpha(\varphi_{h_1h_2}(n)) &= s(h_1h_2)\alpha(n)s(h_2^{-1}h_1^{-1}) \\
&= s(h_1)s(h_2)\alpha(n)s(h_2^{-1})s(h_1^{-1}) \\
&= s(h_1)\alpha(\varphi_{h_2}(n))s(h_1^{-1}) \\
&= \alpha(\varphi_{h_1}(\varphi_{h_2}(n))).
\end{aligned}$$

Then injectivity of α implies $\varphi_{h_1h_2}(n) = \varphi_{h_1}(\varphi_{h_2}(n))$. We conclude that φ_h is bijective with inverse $\varphi_h^{-1} = \varphi_{h^{-1}}$, and moreover that the function $\varphi : H \to \mathrm{Aut}(N)$ defined by $h \mapsto \varphi_h$ is a homomorphism.

Since φ is a homomorphism we can define the semi-direct product $N \rtimes_\varphi H$ as in HW2 Problem 6. Now define the function $\gamma : N \rtimes_\varphi H \to G$ by $\gamma(n,h) = \alpha(n)s(h)$. Clearly this function commutes with the identity maps $\mathrm{id}_N : N \to N$ and $\mathrm{id}_H : H \to H$ since $\gamma(n, 1_H) = \alpha(n)s(1_H) = \alpha(n) = \alpha(\mathrm{id}_N(n))$ and $\gamma(1_N, h) = \alpha(1_N)s(h) = s(h) = s(\mathrm{id}_H(h))$.

I claim that γ is in fact a group isomorphism. To see that it is a homomorphism, consider any $(n_1, h_1), (n_2, h_2) \in N \rtimes_\varphi H$ and note that

$$\begin{aligned}
\gamma((n_1, h_1) \bullet (n_2, h_2)) &= \gamma(n_1 \varphi_{h_1}(n_2), h_1 h_2) \\
&= \alpha(n_1 \varphi_{h_1}(n_2)) s(h_1 h_2) \\
&= \alpha(n_1) \alpha(\varphi_{h_1}(n_2)) s(h_1) s(h_2) \\
&= \alpha(n_1) s(h_1) \alpha(n_2) s(h_1^{-1}) s(h_1) s(h_2) \\
&= \alpha(n_1) s(h_1) \alpha(n_2) s(h_2) \\
&= \gamma(n_1, h_1) \gamma(n_2, h_2).
\end{aligned}$$

To show that γ is surjective, pick $g \in G$. We want to show that there exist $n \in N$ and $h \in H$ such that $g = \gamma(n, h) = \alpha(n) s(h)$. Applying β to both sides gives

$$\beta(g) = \beta(\alpha(n) s(h)) = \beta(\alpha(n)) \beta(s(h)) = 1_H \cdot h = h.$$

So define $h := \beta(g)$. Now we are looking for $n \in N$ such that

$$\begin{aligned}
g &= \alpha(n) s(\beta(g)) \\
s(\beta(g))^{-1} g &= \alpha(n) \\
s(\beta(g^{-1})) g &= \alpha(n).
\end{aligned}$$

Since $\ker \beta \subseteq \operatorname{im} \alpha$, we will be done if we can show that $s(\beta(g^{-1})) g \in \ker \beta$. And, indeed, we have

$$\begin{aligned}
\beta(s(\beta(g^{-1})) g) &= \beta(s(\beta(g^{-1}) g) \\
&= \beta(s(\beta(g^{-1}))) \beta(g) \\
&= \beta(g^{-1}) \beta(g) \\
&= 1_H.
\end{aligned}$$

Finally, to show that γ is injective, suppose we have $n \in N$ and $h \in H$ such that $\gamma(n, h) = \alpha(n) s(h) = 1_G$. Applying β to both sides gives

$$\begin{aligned}
\beta(\alpha(n) s(h)) &= \beta(1_G) \\
\beta(\alpha(n)) \beta(s(h)) &= 1_H \\
1_H \cdot h &= 1_H \\
h &= 1_H.
\end{aligned}$$

Then since $1_G = \alpha(n) s(h) = \alpha(n) s(1_H) = \alpha(n)$, the injectivity of α shows that $n = 1_N$. We conclude that γ is an isomorphism, and this completes the proof of (1) $\Rightarrow$ (2).

To prove that (2) $\Rightarrow$ (1), suppose that we have a homomorphism $\varphi : H \to \operatorname{Aut}(N)$ and an isomorphism $\gamma : N \rtimes_\varphi H \to G$ such that the given diagram commutes. We define a function $s : H \to G$ by $s(h) := \gamma(1_N, h)$. To show that s is a homomorphism, consider any $h_1, h_2 \in H$. Then we have

$$\begin{aligned}
s(h_1) s(h_2) &= \gamma(1_N, h_1) \gamma(1_N, h_2) \\
&= \gamma((1_N, h_1) \bullet (1_N, h_2)) \\
&= \gamma(1_N \varphi_{h_1}(1_N), h_1 h_2) \\
&= \gamma(1_N, h_1 h_2) \\
&= s(h_1 h_2).
\end{aligned}$$

Finally, the commutativity of the right square shows that $\beta(s(h)) = h$ for all $h \in H$. $\square$