200A Homework 4

James Harbour

October 16, 2025

Problem 1

Suppose D_{2n} is a dihedral group. Prove that there exists a splitting short exact sequence of the form

$$1 \to C_n \to D_{2n} \to C_2 \to 1,$$

where C_k is the cyclic group of order k.

Proof. Consider the group presentation

$$D_{2n} = \langle \sigma, \tau \,|\, \tau\sigma\tau^{-1} = \sigma^{-1}, \tau^2 = 1 = \sigma^n \rangle.$$

Let $C = \langle \sigma \rangle \cong C_n$. As $\tau\sigma\tau^{-1} = \sigma^{-1} \in C$, it follows that C is normal in D_{2n}. Moreover, $D_{2n}/C \cong C_2$, so we have a short exact sequence of the above form. It suffices to show now that this sequence splits. To this end we define a map $\psi : D_{2n}/C \to D_{2n}$ by $\psi(\tau C) = \tau$ and $\psi(C) = 1$. This map is a homomorphism and a section of the projection map, so the aforementioned sequence splits. $\square$

Problem 2

Suppose G is a group.

<u>**(a)**</u>: Show that if N_1 and N_2 are normal subgroups of G and $N_1 \cap N_2 = \{1\}$, then for all $x_1 \in N_1$ and $x_2 \in N_2$, $x_1x_2 = x_2x_1$.

Proof. Let $x_1 \in N_1, x_2 \in N_2$. Then $x_2^{-1} \in N_2$, whence $x_1^{-1}x_2^{-1}x_1 \in N_2$ and consequently $x_1^{-1}x_2^{-1}x_1x_2 \in N_2$. On the other hand, $x_2^{-1}x_1x_2 \in N_1$ whence $x_1^{-1}(x_2^{-1}x_1x_2) \in N_1$. Hence, $x_1^{-1}x_2^{-1}x_1x_2 = 1$, so $x_1x_2 = x_2x_1$. $\square$

<u>**(b)**</u>: Suppose $N_1, \ldots, N_k$ are normal subgroups of G and $N_i \cap N_j = \{1\}$ for all $i \neq j$. Prove that

$$f : \prod_{i=1}^{k} N_i \to N_1 \cdots N_k, \qquad f(x_1, \ldots, x_k) := x_1 \cdots x_k$$

is a group homomorphism.

Proof. Note that by part (a), N_i commutes with N_j for $i \neq j$. Thus, we compute

$$f(x_1, \ldots, x_k)f(y_1, \ldots, y_k) = x_1 \cdots x_k y_1 \cdots y_k = x_1y_1x_2x_3 \cdots x_k y_2 \cdots y_k = \cdots = x_1y_1 \cdots x_ky_k = f(x_1y_1, \ldots, x_ky_k),$$

so f is a group homomorphism. $\square$

(c): Suppose $N_1, \ldots, N_k$ are normal subgroups of G, and for all i,

$$N_i \cap N_1 \cdots N_{i-1} N_{i+1} \cdots N_k = \{1\}.$$

Prove that

$$f : \prod_{i=1}^{k} N_i \to N_1 \cdots N_k, \qquad f(x_1, \ldots, x_k) := x_1 \cdots x_k$$

is a group isomorphism.

Proof. It is clear that f is surjective, so it suffices to show the kernel is trivial. Let $x_1, \ldots, x_k$ be such that $f(x_1, \ldots, x_k) = 1$. Then $x_1 \cdots x_k = 1$, whence $x_2 \cdots x_k = x_1^{-1} \in N_1 \cap N_2 N_3 \cdots N_k = \{1\}$ and consequently $x_1 = 1$. Thus $x_2 x_3 \cdots x_k = 1$. Continuing in this way, we obtain that $x_2 = 1$, $x_3 = 1$, and so on until $x_k = 1$. Thus $(x_1, \ldots, x_k) = (1, 1, \ldots 1)$ is trivial. □

Problem 3

Suppose in a finite group G every proper subgroup H satisfies $H \subsetneq N_G(H)$.

(a): Prove that all the Sylow subgroups of G are normal. Deduce that for all prime divisors of $|G|$, G has a unique Sylow p-subgroup.

Proof. Suppose that p is a prime divisor of $|G|$ and $P \in \mathrm{Syl}_p(G)$. Then noting that $N_G(N_G(P)) = N_G(P)$, it follows that $N_G(P)$ is not a proper subgroup of G, so $N_G(P) = G$ whence $P \triangleleft G$. Thus $|\mathrm{Syl}_p(G)| = 1$ for p a prime divisor of $|G|$. □

(b): Prove that

$$G \cong \prod_{p \text{ prime factor of } |G|} P_p,$$

where P_p is the unique Sylow p-subgroup of G.

Proof. Suffices to show

$$P_p \cap \prod_{\substack{q \text{ prime factor of } |G| \\ q \neq p}} P_q = 1 \quad \text{for all } q \text{ prime divisor of } |G|.$$

If $x \neq 1$ and x is in this intersection, then $o(x) = p^k$ for some $k \in \mathbb{N}$. On the other hand, $o(x)$ divides $\prod_{q \neq p} q^{\nu_q(|G|)}$, whence by Euclid's lemma p divides q for some $q \neq p$, which is absurd. Thus by 2(c), we have a group isomorphism $P_{p_1} \cdots P_{p_s} \cong \prod_{p \text{ prime factor of } |G|} P_p$. It suffices to show that the left side of this isomorphism is all of G; however, this follows from size considerations in the direct product on the right hand side of this isomorphism. □

Problem 4

Suppose G is a finite group and A is a normal abelian subgroup of G. Let $s : G/A \to G$ be a section of the natural projection map; that means for all $h \in G/A$, we choose an element $s(h)$ from the coset h. Alternatively, we can say that $s(h)A = h$.
Notice that if s is a group homomorphism, then the standard short exact sequence

$$1 \to A \to G \to G/A \to 1$$

splits. The goal of this exercise is to modify s and make it into a group homomorphism under suitable assumptions.
Let $H := G/A$ and define the function

$$c : H \times H \to A, \qquad c(h_1, h_2) := s(h_1)s(h_2)s(h_1h_2)^{-1}.$$

Notice that since $s(h_1h_2)A = h_1h_2 = s(h_1)As(h_2)A = s(h_1)s(h_2)A$, the image of c is indeed in A. Function c gives us an insight into how far s is from being a group homomorphism.
Since A is abelian, the conjugation action of G on A factors through an action of H. More precisely, for all $h \in H$ and $a \in A$, let

$$h \cdot a := s(h)as(h)^{-1},$$

and notice that this is a well-defined group action.

(a): Prove that, for all $h_1, h_2, h_3 \in H$, we have

$$c(h_1, h_2)c(h_1h_2, h_3) = (h_1 \cdot c(h_2, h_3))c(h_1, h_2h_3).$$

(Since A is abelian, it is more customary to write this in additive notation:

$$c(h_1, h_2) + c(h_1h_2, h_3) = h_1 \cdot c(h_2, h_3) + c(h_1, h_2h_3),$$

and this is called the *2-cocycle relation.*)

Proof. For any $h_1, h_2 \in H$, we may rewrite the definition of $c(h_1, h_2)$ as

$$s(h_1)s(h_2) = c(h_1, h_2)s(h_1h_2).$$

Then for $h_1, h_2, h_3 \in H$, we compute

$$\begin{aligned}(s(h_1)s(h_2))s(h_3) &= c(h_1, h_2)s(h_1h_2)s(h_3) \\ &= c(h_1, h_2)c(h_1h_2, h_3)s(h_1h_2h_3).\end{aligned}$$

On the other hand, grouping differently we observe

$$\begin{aligned}s(h_1)(s(h_2)s(h_3)) &= s(h_1)c(h_2, h_3)s(h_2h_3) \\ &= (s(h_1)c(h_2, h_3)s(h_1)^{-1})s(h_1)s(h_2h_3) \\ &= (h_1 \cdot c(h_2, h_3))s(h_1)s(h_2h_3) \\ &= (h_1 \cdot c(h_2, h_3))c(h_1, h_2h_3)s(h_1h_2h_3).\end{aligned}$$

These two results are equal, so we obtain

$$c(h_1, h_2)c(h_1h_2, h_3)s(h_1h_2h_3) = (h_1 \cdot c(h_2, h_3))c(h_1, h_2h_3)s(h_1h_2h_3),$$

whence cancelling the $s(h_1h_2h_3)$ terms gives

$$c(h_1, h_2)c(h_1h_2, h_3) = (h_1 \cdot c(h_2, h_3))c(h_1, h_2h_3),$$

as desired. $\square$

(b): Prove that the standard short exact sequence

$$1 \to A \to G \to H \to 1$$

splits if and only if there exists a function $b : H \to A$ such that

$$c(h_1, h_2) = b(h_1)(h_1 \cdot b(h_2))b(h_1 h_2)^{-1}.$$

(In additive notation:

$$c(h_1, h_2) = b(h_1) + h_1 \cdot b(h_2) - b(h_1 h_2),$$

called a *2-coboundary.*)

Proof. We first show that splitting is equivalent to there existing a function $b : H \to A$ such that $\psi(h) := b(h)^{-1}s(h)$ is a group homomorphism.

Suppose that the sequence splits. Then there is some group homomorphism $f : H \to G$ such that $f(h)A = h$. But then taking inverses, we have $f(h)^{-1}A = h^{-1} = s(h)^{-1}A$. Let $b : H \to A$ be given by $b(h) := s(h)f(h)^{-1}$. Then $f(h) = b(h)^{-1}s(h)$ which is a group homomorphism by assumption.

On the other hand, suppose that there is some function $b : H \to A$ such that $\psi(h) := b(h)^{-1}s(h)$ is a group homomorphism. Then we compute

$$\psi(h)^{-1}A = s(h)^{-1}b(h)A = s(h)^{-1}A = (s(h)A)^{-1} = h^{-1},$$

whence $\psi(h)A = h$, so ψ is also a section of the projection map from G to H, thus the short exact sequence splits.

Now we compute

$$\begin{aligned}
\psi(h_1)\psi(h_2)\psi(h_1h_2)^{-1} &= b(h_1)^{-1}s(h_1)b(h_2)^{-1}s(h_2)s(h_1h_2)^{-1}b(h_1h_2) \\
&= b(h_1)^{-1}(s(h_1)b(h_2)^{-1}s(h_1)^{-1})s(h_1)s(h_2)s(h_1h_2)^{-1}b(h_1h_2) \\
&= b(h_1)^{-1}(h_1 \cdot b(h_2))^{-1}c(h_1, h_2)b(h_1h_2)
\end{aligned}$$

Thus, ψ is a group homomorphism if and only if

$$1 = \psi(h_1)\psi(h_2)\psi(h_1h_2)^{-1} = b(h_1)^{-1}(h_1 \cdot b(h_2))^{-1}c(h_1, h_2)b(h_1h_2)$$

which holds if and only if

$$c(h_1, h_2) = (h \cdot b(h_2))b(h_1)b(h_1h_2)^{-1}.$$

Thus, the above short exact sequence splits if and only if c is a 2-coboundary.

□

(c): In the above setting, assume that $\gcd(|A|, |H|) = 1$. Prove that every 2-cocycle is a 2-coboundary. Deduce that the standard short exact sequence

$$1 \to A \to G \to H \to 1$$

splits.

Proof. By Bezout, there exist $r, s \in \mathbb{Z}$ such that $1 = r|H| + s|A|$. For $a \in A$, we have

$$a = (r|H| + s|A|) \cdot a = r|H| \cdot a = |H| \cdot (r \cdot a),$$

so setting $y := r \cdot a$ gives $a = |H| \cdot y$. To see that y is unique, suppose that $a \in A$ and $x, y \in A$ are such that $|H| \cdot x = a = |H| \cdot y$. Then $|H| \cdot (x - y) = 0$, whence $o(x - y) \mid |H|$. By Lagrange's theorem, $o(x - y) \mid |A|$, whence by assumption $o(x - y) = 1$, so $x = y$. Let this unique y be denoted $\frac{a}{|H|}$.

Suppose that $c : H \to A$ is a 2-cocycle and let

$$b : H \to A, \quad b(x) := \frac{1}{|H|} \sum_{h \in H} c(x, h).$$

Fix $h_1, h_2 \in H$. Then for $h \in H$, we have

$$c(h_1, h_2) + c(h_1 h_2, h) = h_1 \cdot c(h_2, h) + c(h_1, h_2 h).$$

Summing this equation over $h \in H$, we obtain

$$\begin{aligned}
\sum_{h \in H} c(h_1, h_2) + c(h_1 h_2, h) &= \sum_{h \in H} h_1 \cdot c(h_2, h) + c(h_1, h_2 h) \\
|H| c(h_1, h_2) + \sum_{h \in H} c(h_1 h_2, h) &= h_1 \cdot \sum_{h \in H} c(h_2, h) + \sum_{h \in H} c(h_1, h_2 h) \\
|H| c(h_1, h_2) + |H| b(h_1 h_2) &= |H| (h_1 \cdot b(h_2)) + \sum_{h \in H} c(h_1, h_2 h) \\
&= |H| (h_1 \cdot b(h_2)) + \sum_{h \in H} c(h_1, h) \\
&= |H| (h_1 \cdot b(h_2)) + |H| b(h_1)
\end{aligned}$$

Let $x := (c(h_1, h_2) + b(h_1 h_2) - (h_1 \cdot b(h_2)) - b(h_1))$. Rearranging the above equation gives

$$|H| x = |H| \left(c(h_1, h_2) + b(h_1 h_2) - (h_1 \cdot b(h_2)) - b(h_1) \right) = 0$$

Thus the order of x has $o(x) \mid |H|$. However, $o(x) || A|$, whence $o(x) = 1$ so $x = 0$. Consequently,

$$c(h_1, h_2) = b(h_1) + h_1 \cdot b(h_2) - b(h_1 h_2),$$

so c is a 2-coboundary. Hence by part (b), the short exact sequence $1 \to A \to G \to H$ splits. □

Problem 5

In this problem you will show that S_6 has an automorphism which is not an inner automorphism.

(a): Show that S_5 has 6 Sylow 5-subgroups.

Proof. By the Sylow theorems, $n_5 \in \{1, 2, 4, 6, 8, 12, 24\}$. As $n_5 \equiv 1 \pmod 5$, $n_5 \neq 2, 4, 8, 12, 24$. Thus $n_5 = 1$ or $n_5 = 6$. If $n_5 = 1$, then we have an order 5 normal subgroup $N \triangleleft S_5$, whence $[S_5 : N] = 12 > 2$ contradicting the fact that no such subgroups exist. Thus, $n_5 = 6$. □

(b): Use the action of S_5 on $\mathrm{Syl}_5(S_5)$ and show that S_6 has a subgroup H which is isomorphic to S_5 and for every $\sigma \in S_6$, $\mathrm{Fix}(\sigma H \sigma^{-1}) = \varnothing$, where S_6 acts on $\{1, \ldots, 6\}$.

Proof. Let $S_5 \curvearrowright \mathrm{Syl}_5(S_5)$ by conjugation. This furnishes a homomorphism $\Phi : S_5 \to \mathrm{Sym}(\mathrm{Syl}_5(S_5)) \cong S_6$. Suppose, for the sake of contradiction, that $\ker(\Phi) > 1$. As the action of S_5 on $\mathrm{Syl}_5(S_5)$ is transitive and $\mathrm{Syl}_5(S_{5)}$ is not a singleton set, it must hold that $\ker(\Phi) \neq S_5$. Thus $\ker(\Phi) = A_5$. Hence $\mathbb{Z}/2\mathbb{Z} \cong S_5/A_5 \cong \Phi(S_5)$ and $\Phi(S_5) \subseteq S_6$ is a transitive subgroup of S_6, which is impossible.

Thus $\ker(\Phi) = \{1\}$, so $S_5 \cong \Phi(S_5) \cong H \subseteq S_6$, where the isomorphism $\Phi(S_5) \cong H$ is given by restricting the relabelling isomorphism $\mathrm{Sym}(\mathrm{Syl}_5(S_5)) \cong S_6$. Let $\sigma \in S_6$ and suppose, for the sake of contradiction, that some $1 \leq i \leq 6$ has $i \in \mathrm{Fix}(\sigma H \sigma^{-1})$. Letting $S_6 \curvearrowright \mathrm{Syl}_5(S_5) := \{P_1, \ldots, P_6\}$ in the natural way by relabelling, it follows that $P_i \in \mathrm{Fix}(\sigma \Phi(S_5) \sigma^{-1})$.
Let $x \in S_5$. Then

$$P_i = (\sigma \Phi(x) \sigma^{-1}) \cdot P_i = (\sigma \Phi(x)) \cdot P_{\sigma^{-1}(i)} = \sigma \cdot (x P_{\sigma^{-1}(i)} x^{-1})$$

whence after acting on both sides by σ^{-1}, we obtain

$$P_{\sigma^{-1}(i)} = \sigma^{-1} \cdot P_i = \sigma^{-1} \cdot \sigma \cdot (x P_{\sigma^{-1}(i)} x^{-1}) = x P_{\sigma^{-1}(i)} x^{-1}.$$

This implies that $P_{\sigma^{-1}(i)}$ is a normal subgroup of S_5 of order 5, which does not exist and is thus a contradiction. Thus, for all $\sigma \in S_6$, $\mathrm{Fix}(\sigma H \sigma^{-1}) = \emptyset$. □

(c): Consider the action $S_6 \curvearrowright S_6/H$ by left translations. Argue that this action induces a group homomorphism

$$\theta : S_6 \to S_6.$$

Prove that $\mathrm{Fix}(\theta(H)) \neq \varnothing$.

Proof. The set S_6/H has size 6, so the left translation action $S_6 \curvearrowright S_6/H$ induces a homomorphism $\theta : S_6 \to \mathrm{Sym}(S_6/H) \cong S_6$. Noting that $H \in S_6/H$, observe that for $\rho \in H$, $\theta(\rho) \cdot H = \rho H = H$, so $H \in Fix(\theta(H))$ (or at least the corresponding label in $\{1, \ldots, 6\}$. □

(d): Deduce that $\mathrm{Aut}(S_6) \neq \mathrm{Inn}(S_6)$.

Proof. Suppose that $\sigma \in S_6$ and let $c_\sigma \in \mathrm{Inn}(S_6)$ be given by $c_\sigma(x) = \sigma x \sigma^{-1}$. Then by part (b), $\mathrm{Fix}(c_\sigma(H)) = \mathrm{Fix}(\sigma H \sigma^{-1}) = \emptyset$. Hence, the homomorphism θ in part (c) cannot be inner. Thus, it suffices to show that $\theta \in \mathrm{Aut}(S_6)$.

Note that the action $S_6 \curvearrowright S_6/H$ is transitive and thus $|\theta(S_6)| > 2$. Hence, $[S_6 : \ker(\theta)] = |\theta(S_6)| > 2$, whence $\ker(\theta) = \{1\}$. As the domain and codomain of θ are both finite and of the same size, the injectivity of θ implies the surjectivity of θ, whence θ is an automorphism of S_6.

□

Problem 6

Prove that a group of order 36 is not simple.

Proof. Let G be a group of order 36. Suppose, for the sake of contradiction, that G is simple. Note that $|G| = 36 = 2^2 3^2$. By simplicity, $n_2, n_3 \neq 1$, so Sylow's theorems give

$$\begin{aligned} n_2 &\in \{3, 3^2\} \quad n_2 \equiv 1 \pmod 2 \\ n_3 &\in \{2, 2^2\} \quad n_3 \equiv 1 \pmod 3. \end{aligned}$$

As $2 \not\equiv 1 \pmod 3$, it follows that $n_3 = 2^2 = 4$. Consider the conjugation action $G \curvearrowright \mathrm{Syl}_3(G)$. This furnishes a homomorphism $\Phi : G \to S_4$. Suppose, for the sake of contradiction, that $\ker(\Phi) = \{1\}$. Then G embeds into S_4. Fix $P \in \mathrm{Syl}_3(G)$. Then P embeds into S_4, whence by Lagrange's theorem $9 = |P| \mid |S_4| = 24$, which is a contradiction. Thus $\ker(\Phi) \neq \{1\}$. However, as G acts transitively on $\mathrm{Syl}_3(G)$ and $|\mathrm{Syl}_3(G)| > 1$, it must hold that $\ker(\Phi)$ is a proper subgroup of G. Thus $\ker(\Phi)$ is a nontrivial, proper, normal subgroup of G, which contradicts simplicity. $\square$

Problem 7

Suppose N and H are two groups and $f_1, f_2 : H \to \mathrm{Aut}(N)$ are two group homomorphisms.
<u>**(a)**</u>: Suppose $\theta : N \rtimes_{f_1} H \to N \rtimes_{f_2} H$ is an isomorphism such that the following diagram commutes:

$$\begin{array}{ccccccc} 1 & \to & N & \to & N \rtimes_{f_1} H & \to H \to 1 \\ 1 & \to & N & \to & N \rtimes_{f_2} H & \to H \to 1 \end{array}$$

with vertical maps id_N, θ, and id_H. Let $\sigma : H \to \mathrm{Aut}(N)$ be defined by $\sigma(h) := f_2(h) \circ f_1(h)^{-1}$. Prove that $\sigma(h)$ is an inner automorphism of N for all $h \in H$.

Proof. Multiplication in $N \rtimes_f H$

$$(n, h)(n', h') = (nf(h)(n'), hh')$$

Let $\pi_j : N \rtimes_{f_j} H \to H$ denote the projection homomorphisms in the above diagram for $j = 1, 2$. Then by commutativity we note that $id_H \circ \pi_H^1 = \pi_H^2 \circ \theta$, whence for $h \in H$ we have

$$h = id_H(\pi_H^1(1, h)) = \pi_H^2(\theta(1, h)).$$

For $h \in H$, there exists some $n(h) \in N$ such that $\theta(1, h) = (n(h), h)$. This gives a function $n : H \to N$.

Let $\iota_N^j : N \to N \rtimes_{f_j} H$ denote the inclusion maps in the above diagram for $j = 1, 2$. Then by commutativity, we note that $\theta \circ \iota_N^1 = \iota_N^2 \circ id_N$, whence for $n \in N$ we have

$$\theta(n, 1) = \theta \circ \iota_N^1(n) = \iota_N^2 \circ id_N(n) = (n, 1) \in N \rtimes_{f_2} H,$$

whence we see

$$\theta(n, h) = \theta((n, 1) \cdot (1, h)) = \theta(n, 1) \cdot \theta(1, h) = (n, 1) \cdot (n(h), h) = (n \cdot n(h), h).$$

Note that $(n, h)^{-1} = (f_j(h)^{-1}(n^{-1}), h^{-1})$ inside $N \rtimes_{f_j} H$. Now we compute the quantity $\theta((1, h) \cdot (n, 1) \cdot (1, h)^{-1})$ two separate ways. On one hand, we have

$$\begin{aligned} \theta((1, h) \cdot (n, 1) \cdot (1, h)^{-1}) &= \theta(1, h)\theta(n, 1)\theta(1, h)^{-1} \\ &= (n(h), h) \cdot (n, 1) \cdot (n(h), h)^{-1} \\ &= (n(h)f_2(h)(n), h) \cdot (f_2(h)^{-1}(n(h)^{-1}), h^{-1}) \\ &= (n(h)f_2(h)(n)f_2(h)(f_2(h)^{-1}(n(h)^{-1})), 1) \\ &= (n(h)f_2(h)(n)n(h)^{-1}, 1). \end{aligned}$$

On the other hand, performing multipication inside θ first, we see that

$$\begin{aligned}\theta((1,h)\cdot(n,1)\cdot(1,h)^{-1}) &= \theta((f_1(h)(n),h)\cdot(1,h^{-1}))\\ &= \theta((f_1(h)(n),1))\\ &= (f_1(h)(n),1).\end{aligned}$$

Thus, as we computed the same quantities, we must have

$$f_1(h)(n) = n(h)f_2(h)(n)n(h)^{-1}.$$

For $g \in N$, let $c_g \in Inn(N)$ denote the inner automorphism given by $c_g(x) = gxg^{-1}$. Then, observe that

$$\sigma(h)^{-1}(n) = f_1(h)(f_2(h)^{-1}(n)) = n(h)f_2(h)(f_2(h)^{-1}(n))n(h)^{-1} = n(h)\cdot n\cdot n(h)^{-1} = c_{n(h)}(n),$$

whence $\sigma(h)^{-1} = c_{n(h)}$ and consequently $\sigma(h) = (c_{n(h)})^{-1} = c_{n(h)^{-1}}$ is an inner automorphism. □

(b): In the setting of part (a), prove that

$$\sigma(h_1h_2) = \sigma(h_1)\circ f_1(h_1)\circ\sigma(h_2)\circ f_1(h_1)^{-1}.$$

Proof. Noting that the maps $f_j : H \to \mathrm{Aut}(N)$ are group homomorphisms, we compute

$$\begin{aligned}\sigma(h_1)\circ f_1(h_1)\circ\sigma(h_2)\circ f_1(h_1)^{-1} &= f_2(h_1)\circ f_1(h_1)^{-1}\circ f_1(h_1)\circ f_2(h_2)\circ f_1(h_2)^{-1}\circ f_1(h_1)^{-1}\\ &= f_2(h_1)\circ f_2(h_2)\circ f_1(h_2)^{-1}\circ f_1(h_1)^{-1}\\ &= f_2(h_1h_2\circ(f_1(h_1)\circ f_1(h_2))^{-1}\\ &= f_2(h_1h_2\circ f_1(h_1h_2)^{-1}\\ &= \sigma(h_1h_2).\end{aligned}$$

□

(c): Suppose there exists $\theta \in \mathrm{Aut}(H)$ such that $f_1 = f_2\circ\theta$. Prove that there exists an isomorphism $\Theta : N \rtimes_{f_1} H \cong N \rtimes_{f_2} H$ such that the following diagram commutes:

$$\begin{array}{ccccccccc}1 & \to & N & \to & N\rtimes_{f_1} H & \to & H & \to & 1\\ 1 & \to & N & \to & N\rtimes_{f_2} H & \to & H & \to & 1\end{array}$$

with vertical maps id_N, Θ, and θ.

Proof. Define $\overline{\theta}(n,h) := (n,\theta(h))$.

$$\begin{aligned}\overline{\theta}((n_1,h_1)(n_2,h_2)) &= \overline{\theta}(n_1f_1(h_1)(n_2),h_1h_2)\\ &= (n_1f_1(h_1)(n_2),\theta(h_1h_2))\end{aligned}$$

On the other hand, using that $f_1 = f_2\circ\theta$, we see

$$\begin{aligned}\overline{\theta}(n_1,h_1)\overline{\theta}(n_2,h_2) &= (n_1,\theta(h_1))\cdot(n_2,\theta(h_2))\\ &= (n_1f_2(\theta(h_1)(n_2),\theta(h_1)\theta(h_2))\\ &= (n_1f_1(h_1)(n_2),\theta(h_1h_2)),\end{aligned}$$

whence it follows that $\overline{\theta}$ is indeed a group homomorphism.

Suppose that $(n,h) \in N \rtimes_{f_2} H$. As θ is an automorphism, we have

$$\overline{\theta}(n, \theta^{-1}(h)) = (n, \theta \circ \theta^{-1}(h)) = (n,h),$$

whence $\overline{\theta}$ is surjective.

Now suppose that $(n,h) \in \ker(\overline{\theta})$. Then

$$(1_N, 1_H) = \overline{\theta}(n,h) = (n, \theta(h)),$$

whence $n = 1_N$ and $h \in \ker(\theta) = \{1_H\}$, so $h = 1_H$. Thus $\overline{\theta}$ is also injective, and is consequently an isomorphism.

For $n \in N$, we see that

$$\overline{\theta} \circ \iota_N^1(n) = \overline{\theta}(n,1) = (n,1) = \iota_N^2 \circ id_N(n)$$

so $\overline{\theta} \circ \iota_N^1 = \iota_N^2 \circ id_N$. For $(n,h) \in N \rtimes_{f_1} H$, we compute

$$\pi_H^2 \circ \overline{\theta}(n,h) = \pi_H^2(n, \theta(h)) = \theta(h) = \theta(\pi_H^1(n,h)),$$

whence $\pi_H^2 \circ \overline{\theta} = \theta \circ \pi_H^1$. Thus we have shown that the above diagram commutes.

$\square$