MTH 644 Homework 4

Noah Prentice

11 March 2024

Contents

Exercise 1. Show that up to isomorphism there are exactly four groups of order 28. [Hint: Use Sylow's Theorem and semi-direct products.]

Proof. Let G be a group of order $28 = 2^2 \cdot 7$. By Sylow's Theorem (3), the number of Sylow 7-subgroups of G, n_7, is congruent to 1 modulo 7, and so this number belongs to the set $\{1, 8, 15, \ldots\}$. Also by Sylow's Theorem (3), this number properly divides $2^2 = 4$, and hence belongs to the set $\{1, 2, 4\}$. The only number that satisfies this property is 1, so G has a unique Sylow 7-subgroup H. By Sylow's Theorem (2), this implies that H is a normal subgroup of G.

By Sylow's Theorem (1), G has a Sylow 2-subgroup, K, and thus K has order 4. Now we claim that $H \cap K = \{e\}$: if $a \in H \cap K$, then, by Lagrange's Theorem, the order of a properly divides the order of H (as a is an element of H) and the order of a properly divides the order of K. Since the order of H is 7 and the order of K is 4, and since the only positive number that is a proper divisor of both 7 and 4 is 1, this implies that the order of a is 1, hence a is the identity element. Thus G is the semidirect product of H and K by Theorem 12 in Section 5.5.

Since H has prime order, it is cyclic by Cauchy's Theorem. By Proposition 16 in Section 4.4, then, the automorphism group of H is isomorphic to $\mathbb{Z}_7^\times$. Note then that $\mathbb{Z}_7^\times$ is a cyclic group of order 6: $\langle 3 \rangle = \{3, 3^2, 3^3, 3^4, 3^5, 3^6\} = \{3, 2, 6, 4, 5, 1\}$ where this multiplication is done modulo 7. Therefore the automorphism group of H is isomorphic to $\mathbb{Z}_6$, that is, there is some isomorphism f from $\mathbb{Z}_6$ into $\mathrm{Aut}(H)$. So we consider homomorphisms from K into $\mathbb{Z}_6$. Since K has order 4, and since every group of order 4 is either isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$, we can consider two cases:

1. K is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Then K has 3 nonidentity elements of order 2, a, b, and c, and it is generated by any pair of these elements. Let φ be any homomorphism from K into $\mathbb{Z}_6$. Since the orders of $\varphi(a)$, $\varphi(b)$, and $\varphi(a)\varphi(b) = \varphi(ab) = \varphi(c)$ divide the orders of a, b, and c respectively, and since the divisors of 2 are 1 and 2, we can consider 2 subcases:

   (a) The images of two nonidentity elements of K have order 1. Without loss of generality, suppose $\varphi(a)$ and $\varphi(b)$ have order 1. Then,, since $K = \langle a, b \rangle$, $\varphi : K \to \mathbb{Z}_6$ is the trivial homomorphism, and hence $f \circ \varphi : K \to \mathrm{Aut}(H)$ is also the trivial homomorphism. This yields $G \cong H \rtimes_{f \circ \varphi} K = H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_7 \cong \mathbb{Z}_2 \times \mathbb{Z}_{14}$.

   (b) The images of two nonidentity elements of K have order 2. Without loss of generality, suppose $\varphi(a)$ and $\varphi(b)$ have order 2. Because 3 is the unique element of $\mathbb{Z}_6$ with order 2, this implies that $f \circ \varphi(a) = f \circ \varphi(b)$ is the unique element of $\mathrm{Aut}(H)$ that has order 2, namely the inversion map. Thus, in particular, $f \circ \varphi$ is not the trivial homomorphism from K into $\mathrm{Aut}(H)$. By part (3) of Proposition 11 in Section 5.5, then, K is not a normal subgroup of $G = H \rtimes_{f \circ \varphi} K$, and so G is non-abelian.

   Now we show that G has no elements of order 4. Suppose that (h, k) is an element of G such that $(h, k)^4 = e_G$. Then note that $k^2 = e_K$ as every element of K has order 1 or 2. So

$$\begin{aligned}
[(h,k)(h,k)][(h,k)(h,k)] &= (h \cdot f \circ \varphi(k)(h), k^2)(h \cdot f \circ \varphi(k)(h), k^2) \\
&= (h \cdot f \circ \varphi(k)(h), e_K)(h \cdot f \circ \varphi(k)(h), e_K) \\
&= \big(h \cdot f \circ \varphi(k)(h) \cdot f \circ \varphi(e_K)(h \cdot f \circ \varphi(k)(h)), e_K\big) \\
&= \big(h \cdot f \circ \varphi(k)(h) \cdot h \cdot f \circ \varphi(k)(h), e_K\big)
\end{aligned}$$

Now, if $k = a$ or $k = b$, then $f \circ \varphi(k)(h) = h^{-1}$. In this case, $(h,k)^2 = (h \cdot h^{-1}, k^2) = (e_H, e_K)$ (as $a^2 = b^2 = e_K$), and so (h,k) has order 1 or 2. In particular, then, (h,k) does not have order 4. If, instead, $k = e_K$ or $k = ab = c$, then $f \circ \varphi(k)$ has order one by the construction above, and hence $f \circ \varphi(k)(h) = h$. In this case, $(h,k)^4 = (h^4, k^4)$. So, if $(h,k)^4 = e_G$, then in particular $h^4 = e_H$. By Lagrange's Theorem, the order of h therefore divides 4 and 7, and thus h has order 1, and therefore $h = e_H$. In this case, again, $(h,k)^2 = (e_H, k^2) = (e_H, e_K)$ as $e_K^2 = c^2 = e_K$. This implies that (h,k) has order 1 or 2, and so in particular (h,k) does not have order 4. This therefore proves that no element of G has order 4.

2. K is isomorphic to $\mathbb{Z}_4$. Then K is cyclic and generated by an element $k \in K$. Let φ be any homomorphism from K into $\mathbb{Z}_6$. Since the order of $\varphi(k)$ divides the order of k, which is 4, $\varphi(k)$ must be an element of $\mathbb{Z}_6$ with order 1, 2, or 4. Because $\mathbb{Z}_6$ contains no elements of order 4, $\varphi(k)$ has order 1 or 2. We consider now these two subcases:

   (a) $\varphi(k)$ has order 1. Then, because k is a generator of K, $\varphi(K) = 0$ and so φ is the trivial homomorphism. This yields the trivial homomorphism $f \circ \varphi$ from K into $\mathrm{Aut}(H)$, in which case $G \cong H \rtimes_{f \circ \varphi} K = H \times K \cong \mathbb{Z}_{28}$.

   (b) $\varphi(k)$ has order 2. In this case, $f \circ \varphi$ is a homomorphism from K into $\mathrm{Aut}(H)$ that maps k to the unique element of $\mathrm{Aut}(H)$ with order 2, namely the inversion map. In particular, then, $f \circ \varphi$ is not the trivial homomorphism from K into $\mathrm{Aut}(H)$. By part (3) of Proposition 11 in Section 5.5, then, K is not a normal subgroup of $G = H \rtimes_{f \circ \varphi} K$, and so G is non-abelian. Furthermore, consider the element (e_H, k) in G:

$$\begin{aligned}
(e_H, k)^4 &= [(e_H, k)(e_H, k)][(e_H, k)(e_H, k)] \\
&= (e_H \ f \circ \varphi(k)(e_H), k^2)(e_H f \circ \varphi(k)(e_H), k^2) \\
&= (e_H, k^2)(e_H, k^2) \\
&= (e_H \ f \circ \varphi(k^2)(e_H), k^4) \\
&= (e_H, k^4) \\
&= (e_H, e_K) \\
&= e_{G_2}.
\end{aligned}$$

   Thus, since $k^2 \neq e_K$, (e_H, k) has order 4.

The above shows that there are at most 4 groups of order 28. Furthermore, we have that

1. The two abelian groups are nonisomorphic as $\mathbb{Z}_{28}$ has an element of order 28 while $\mathbb{Z}_2 \times \mathbb{Z}_{14}$ does not.
2. The two non-abelian groups are nonisomorphic as G_1 has no elements of order 4 while G_2 has an element of order 4.
3. No abelian group is isomorphic to a non-abelian group.

Therefore the 4 groups constructed are distinct. We conclude that there are, up to isomorphism, exactly 4 groups of order 28. □

Exercise 2 (Dummit and Foote p. 184 #6)**.** Assume that K is a cyclic group, H is an arbitrary group and φ_1 and φ_2 are homomorphisms from K into $\mathrm{Aut}(H)$ such that $\varphi_1(K)$ and $\varphi_2(K)$ are conjugate subgroups of $\mathrm{Aut}(H)$. If K is infinite assume φ_1 and φ_2 are injective. Prove by constructing an explicit isomorphism that $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$ (in particular, if the subgroups $\varphi_1(K)$ and $\varphi_2(K)$ are equal in $\mathrm{Aut}(H)$, then the resulting semidirect products are isomorphic). [Suppose $\sigma\varphi_1(K)\sigma^{-1} = \varphi_2(K)$ so that for some $a \in \mathbb{Z}$ we have $\sigma\varphi_1(k)\sigma^{-1} = \varphi_2(k)^a$ for all $k \in K$. Show that the map $\psi : H \rtimes_{\varphi_1} K \to H \rtimes_{\varphi_2} K$ defined by $\psi((h,k)) = (\sigma(h), k^a)$ is a homomorphism. Show ψ is bijective by constructing a 2-sided inverse.]

Proof. If $\varphi_1(K)$ and $\varphi_2(K)$ are conjugate subgroups of $\mathrm{Aut}(H)$, then there exists an element σ of $\mathrm{Aut}(H)$ such that $\sigma\varphi_1(K)\sigma^{-1} = \varphi_2(K)$. Since K is cyclic, it is generated by some element k. Then $\sigma\varphi_1(k)\sigma^{-1} \in \varphi_2(K)$, so there is some element $q \in K$ such that $\sigma\varphi_1(k)\sigma^{-1} = \varphi_2(q)$. But, because k generates K, $q = k^a$ for some integer a. We now make and prove a subclaim.

Subclaim 2.1.

For all $g \in K$, $\sigma\varphi_1(g)\sigma^{-1} = \varphi_2(g)^a$.

Proof of subclaim 2.1.

Let $g \in K$ be given arbitrarily. Then, because k generates K, $g = k^n$ for some integer n. Thus

$$\begin{aligned}
\sigma\varphi_1(g)\sigma^{-1} &= \sigma\varphi_1(k^n)\sigma^{-1} \\
&= \sigma\varphi_1(k)^n\sigma^{-1} \quad \text{as } \varphi_1 \text{ is a homomorphism} \\
&= (\sigma\varphi_1(k)\sigma^{-1})^n \\
&= \varphi_2(k^a)^n \\
&= \varphi_2(k^n)^a \quad \text{as } \varphi_2 \text{ is a homomorphism} \\
&= \varphi_2(g)^a.
\end{aligned}$$

Since this is true for an arbitrary element of K, it is true for all elements of K, proving the result. □

We use this fact to motivate the construction of the following function, which we will then show to be an isomorphism.

Definition.

Define $\psi : H \rtimes_{\varphi_1} K \to H \rtimes_{\varphi_2} K$ as $\psi\big((h,k)\big) = \big(\sigma(h), k^a\big)$.

We will make a series of subclaims showing that ψ is an isomorphism.

Subclaim 2.2.

ψ is a homomorphism.

Proof of subclaim 2.2.

Let (h_1, k_1), (h_2, k_2) be arbitrary elements of $H \rtimes_{\varphi_1} K$. Then

$$\begin{aligned}
\psi\big((h_1,k_1)(h_2,k_2)\big) &= \psi\big((h_1 \cdot \varphi_1(k_1)(h_2), k_1k_2)\big) \\
&= \Big(\sigma\big(h_1 \cdot \varphi_1(k_1)(h_2)\big), (k_1k_2)^a\Big) \\
&= \Big(\sigma(h_1) \cdot \big(\sigma \circ \varphi_1(k_1)\big)(h_2), (k_1k_2)^a\Big) && \text{as } \sigma \text{ is a homomorphism} \\
&= \Big(\sigma(h_1) \cdot \big(\varphi_2(k_1)^a \sigma\big)(h_2), (k_1k_2)^a\Big) && \text{by claim above} \\
&= \Big(\sigma(h_1) \cdot \varphi_2(k_1^a)\big(\sigma(h_2)\big), (k_1k_2)^a\Big) && \text{as } \varphi_2 \text{ is a homomorphism} \\
&= \Big(\sigma(h_1) \cdot \varphi_2(k_1^a)\big(\sigma(h_2)\big), k_1^a k_2^a\Big) && \text{as } K \text{ is abelian} \\
&= \Big(\sigma(h_1), k_1^a\Big)\Big(\sigma(h_2), k_2^a\Big) \\
&= \psi\big((h_1,k_1)\big)\psi\big((h_2,k_2)\big).
\end{aligned}$$

Thus ψ is a homomorphism, proving subclaim 2.2. □

We now venture to prove that ψ is invertible, which will require several intermediate results.

Subclaim 2.3.

Suppose m and ℓ are integers with $\ell \mid m$. Then the function $f : \mathbb{Z}_m^\times \to \mathbb{Z}_\ell^\times$ which maps every element of $\mathbb{Z}_m^\times$ to its remainder after division by ℓ is surjective.

Proof of subclaim 2.3.

Let $x \in \mathbb{Z}_\ell^\times$ be given arbitrarily, and let $p_1, p_2, \ldots, p_n$ be the primes dividing m but not x. Then define

$$v := \prod_{i=1}^{n} p_i.$$

We will show that $\gcd(x + v\ell, m) = 1$. Suppose p is a prime dividing m, and consider two cases:

(i) <u>p divides x.</u> Then, by construction, $p \notin \{p_i : i \in \{1, 2, \ldots, n\}\}$. Thus implies that p does not divide v. Additionally, since p divides x and $\gcd(x, \ell) = 1$ (as $x \in \mathbb{Z}_\ell^\times$), this implies that p does not divide ℓ. So p divides x but not $v\ell$, and hence p does not divide $x + v\ell$.

(ii) <u>p does not divide x.</u> Then, by construction, p divides v. So p divides $v\ell$ but not x, and hence p does not divide $x + v\ell$.

In both cases above, p does not divide $x + v\ell$, and therefore every prime dividing m does not divide $x + v\ell$, showing that $\gcd(x + v\ell, m) = 1$. Therefore $x + v\ell \in \mathbb{Z}_m^\times$, and

$x + v\ell \equiv x \pmod{\ell}$, so $f(x + v\ell) = x$. Since this is true for an arbitrary element of $\mathbb{Z}_\ell^\times$, it is true for every element of $\mathbb{Z}_\ell^\times$, and hence f is surjective, proving subclaim 2.3. □

We use this result to prove the next subclaim.

Subclaim 2.4.

Suppose K has finite order m. Then there exists an integer b such that $ab \equiv 1 \pmod{m}$.

Proof of subclaim 2.4.

Let $\ell = |\varphi_2(K)|$, and recall several facts:

1. K is generated by k.
2. Homomorphisms map generators to generators of the image: if G_1 is a group generated by g, and if $\zeta : G_1 \to G_2$ is a homomorphism, then $\zeta(G_1)$ is generated by $\zeta(g)$ (see Theorem 4 in Section 2.3).
3. The map defined by conjugation by σ—i.e., $\gamma_\sigma : \mathrm{Aut}(H) \to \mathrm{Aut}(H)$—is a homomorphism.
4. Powers of a generator of a group are themselves generators if and only if the power is relatively prime to the order of the group: if G is a finite group generated by g, then g^a generates G if and only if $\gcd(a, |G|) = 1$ (see Proposition 6 in Section 2.3).

Then, we make several observations:

1. Facts 1-3 imply that $\varphi_2(K)$ is generated by both $\varphi_2(k)$ and $\sigma\varphi_1(k)\sigma^{-1} = \varphi_2(k)^a$.
2. Fact 4 implies that $\gcd(a, \ell) = 1$, and hence $a \in \mathbb{Z}_\ell^\times$. So, by subclaim 2.3, there exists an integer v such that $c = a + v\ell$ is an element of $\mathbb{Z}_m^\times$.
3. By Lagrange's Theorem, $\varphi_2(k)^\ell = e_{\mathrm{Aut}(H)}$.

The above observations reveal that

$$\begin{aligned}
\varphi_2(k)^a &= \varphi_2(k)^{c - v\ell} \\
&= \varphi_2(k)^c \big(\varphi_2(k)^\ell\big)^{-v} \\
&= \varphi_2(k)^c \cdot e_{\mathrm{Aut}(H)}^{-v} \\
&= \varphi_2(k)^c.
\end{aligned}$$

Thus $\gcd(a, m) = \gcd(c, m) = 1$, where this final equality holds from the fact that $c \in \mathbb{Z}_m^\times$. This implies that $a \in \mathbb{Z}_m^\times$, and so there exists an element $b \in \mathbb{Z}_m^\times$ such that $ab \equiv 1 \pmod{m}$, proving subclaim 2.4. □

We can use subclaim 2.4 to finish our proof.

Subclaim 2.5.

ψ is invertible.

Proof of subclaim 2.5.

Suppose first that K is finite with order m. Then, by subclaim 2.4, there exists an integer b such that $ab \equiv 1 \pmod{m}$. In this case define $\xi : H \rtimes_{\varphi_2} K \to H \rtimes_{\varphi_1} K$ by $\xi\big((h,k)\big) = \big(\sigma^{-1}(h), k^b\big)$. Then, for all $(h,k) \in H \times K$,

$$\begin{aligned}
\psi \circ \xi\big((h,k)\big) &= \psi\big((\sigma^{-1}(h), k^b)\big) \\
&= \big(\sigma(\sigma^{-1}(h)), (k^b)^a\big) \\
&= (h,k) \\
&= \big(\sigma^{-1}(\sigma(h)), (k^a)^b\big) \\
&= \xi\big((\sigma(h), k^a)\big) \\
&= \xi \circ \psi\big((h,k)\big).
\end{aligned}$$

Thus $\psi \circ \xi = \xi \circ \psi = \mathrm{id}$, and thus ψ is invertible.

Now suppose that K is infinite, and that, as suggested in the problem statement, φ_1 and φ_2 are injective. Then, because K is an infinite cyclic group, $K \cong \mathbb{Z}$, and so $\varphi_1(K) \cong \varphi_2(K) \cong \mathbb{Z}$ as injective homomorphisms are isomorphisms onto their range. In this case, we make several notes:

1. k generates K.
2. Isomorphisms map generators to generators.
3. The only generators of $\mathbb{Z}$ are 1 and its inverse -1.

The above notes imply that, since $\sigma\varphi_1(k)\sigma^{-1} = \varphi_2(k)^a$, $a = 1$ or $a = -1$. Then calculations similar to those in the finite case show that $\xi : H \rtimes_{\varphi_2} K \to H \rtimes_{\varphi_1} K$ given by $\xi\big((h,k)\big) = \big(\sigma^{-1}(h), k^a\big)$ is an inverse for ψ. □

Combining subclaims 2.2 and 2.5, ψ is an invertible homomorphism from $H \rtimes_{\varphi_1} K$ into $H \rtimes_{\varphi_2} K$, and thus these groups are isomorphic, proving the result. □

Exercise 3 (Dummit and Foote p. 186 #18)**.** Show that if H is any group then there is a group G that contains H as a normal subgroup with the property that for every automorphism σ of H there is an element $g \in G$ such that conjugation by g when restricted to H is the given automorphism σ, i.e., every automorphism of H is obtained as an inner automorphism of G restricted to H.

Proof. Let $G = \mathrm{Hol}(H) = H \rtimes_{\mathrm{id}} \mathrm{Aut}(H)$. Then $H = \{(h, e_{\mathrm{Aut}(H)}) : h \in H\} \trianglelefteq G$ by part (3) of Theorem 10 in Section 5.5. Furthermore, if σ is an automorphism of H, then let $g = (e_H, \sigma)$. Then, for all $h \in H$,

$$\begin{aligned} g(h, e_{\mathrm{Aut}(H)})g^{-1} &= (e_H, \sigma)(h, e_{\mathrm{Aut}(H)})(e_H, \sigma^{-1}) \\ &= (e_H, \sigma)(h\ \sigma^{-1} \cdot e_H, e_{\mathrm{Aut}(H)}\sigma^{-1}) \\ &= (e_H, \sigma)(h, \sigma^{-1}) \\ &= (e_H\sigma \cdot h, \sigma\sigma^{-1}) \\ &= (\sigma(h), e_{\mathrm{Aut}(H)}). \end{aligned}$$

Thus conjugation by g when restricted to H is the automorphism σ. □

Exercise 4 (Dummit and Foote p. 187 #22)**.** Let F be a field, let n be a positive integer, and let G be the group of upper triangular matrices in $\mathrm{GL}_n(F)$ (cf. Exercise 16, Section 2.1).

(a) Prove that G is the semidirect product $U \rtimes D$ where U is the set of upper triangular matrices with 1's down the diagonal and D is the set of diagonal matrices in $\mathrm{GL}_n(F)$.

(b) Let $n = 2$. Recall that $U \cong F$ and $D \cong F^\times \times F^\times$ (cf. Exercise 11 in Section 3.1). Describe the homomorphism from D into $\mathrm{Aut}(U)$ explicitly in terms of these isomorphisms (i.e., show how each element of $F^\times \times F^\times$ acts as an automorphism on F).

Proof.
(a) We proceed towards an application of Theorem 12 in Section 5.5, requiring therefore 3 subclaims. We begin by showing that part (1) of the Theorem holds.

Subclaim 4.1.

U is a normal subgroup of G.

Proof of subclaim 4.1.

Let $u \in U$ and $g \in G$ be given arbitrarily, and let I denote the $n \times n$ identity matrix, that is, the identity element of G. Because u has 1's down the diagonal by construction, $u - I$ is a strictly upper triangular matrix. Let $u^+ = u - I$. Then, because the product of an upper triangular matrix with a strictly upper triangular matrix is strictly upper triangular by results from linear algebra, this implies that gu^+g^{-1} is strictly upper triangular and hence $I + gug^{-1}$ is an element of U. Thus

$$\begin{aligned} gug^{-1} &= g(I + u^+)g^{-1} \\ &= gIg^{-1} + gu^+g^{-1} \\ &= I + gu^+g^{-1} \in U. \end{aligned}$$

Since $u \in U$ and $g \in G$ were arbitrary, this shows that U is a normal subgroup of G, completing subclaim 4.1. □

Now we show that part (2) of the Theorem holds.

Subclaim 4.2.

Let I denote the $n \times n$ identity matrix, that is, the identity element of G. Then $U \cap D = \{I\}$.

Proof of subclaim 4.2.

Suppose $A \in U \cap D$. Since $A \in D$, A's non-diagonal entries are 0. Then, since $A \in U$, A's diagonal entries are 1. Therefore $A = I$, proving subclaim 4.2. □

Subclaims 4.1 and 4.2, along with Theorem 12 in Section 5.5, imply that $U \rtimes D$ is isomorphic to the subgroup UD of G. To complete the proof, we prove the following third subclaim.

Subclaim 4.3.

$G = UD$.

Proof of subclaim 4.3.

Let $g \in G$ be given arbitrarily. For $i \in \{1, 2, \dots, n\}$, define $d_i = g_{ii}$, the ith diagonal element of g. Note that, because g is triangular, $\det(g) = \prod_{i=1}^{n} d_i$, and since $g \in \mathrm{GL}_n(F)$, $\det(g) \neq 0$. This implies that $d_i \neq 0$ for all $i \in \{1, 2, \dots, n\}$. Then, let $u \in U$ be defined as

$$u_{ij} = \begin{cases} 0 & \text{if } i > j \\ 1 & \text{if } i = j \\ g_{ij} d_j^{-1} & \text{if } i < j. \end{cases}$$

Then u is upper triangular and has 1s along the diagonal, so $u \in U$. Furthermore, define $d = (d_i \delta_{ij})$, the matrix whose diagonal elements are the same as those of g and whose non-diagonal elements are 0. Then $d \in D$, and

$$\begin{aligned} ud &= \begin{pmatrix} 1 & g_{12}d_2^{-1} & g_{13}d_3^{-1} & \cdots & g_{1n}d_n^{-1} \\ 0 & 1 & g_{23}d_3^{-1} & \cdots & g_{2n}d_n^{-1} \\ 0 & 0 & 1 & \cdots & g_{3n}d_n^{-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 \\ 0 & 0 & d_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \\ &= \begin{pmatrix} d_1 & g_{12}d_2^{-1}d_2 & g_{13}d_3^{-1}d_3 & \cdots & g_{1n}d_n^{-1}d_n \\ 0 & d_2 & g_{23}d_3^{-1}d_3 & \cdots & g_{2n}d_n^{-1}d_n \\ 0 & 0 & d_3 & \cdots & g_{3n}d_n^{-1}d_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & d_n \end{pmatrix} \\ &= \begin{pmatrix} g_{11} & g_{12} & g_{13} & \cdots & g_{1n} \\ 0 & g_{22} & g_{23} & \cdots & g_{2n} \\ 0 & 0 & g_{33} & \cdots & g_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & g_{nn} \end{pmatrix} \\ &= g, \end{aligned}$$

and thus $g \in UD$. Since this is true for an arbitrary element of G, it is true for all elements of G, and therefore $G \subseteq UD$. Since $UD \subseteq G$, this proves that $G = UD$, completing subclaim 4.3. □

By combining the results of subclaims 4.1, 4.2, and 4.3, Theorem 12 in Section 5.5 implies that $G \cong U \rtimes D$, proving the result.

(b) Recall that the homomorphism φ from D into $\mathrm{Aut}(U)$ that yields the semidirect product from part (a) maps each element d of D to the conjugation map $\gamma_d \in \mathrm{Aut}(U)$. Thus, in terms of the isomorphisms $\psi : D \to F^\times \times F^\times$ and $\theta : U \to F$ in Exercise 11 given by

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \overset{\psi}{\mapsto} (a,b), \qquad \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \overset{\theta}{\mapsto} c,$$

the action of $(a,b) \in F^\times \times F^\times$ on $c \in F$ is given by $(a,b)\cdot c = \theta\Big(\varphi\big(\psi^{-1}\big((a,b)\big)\big)\big(\theta^{-1}(c)\big)\Big)$. In particular, since the action φ in G is given by

$$\begin{aligned} \varphi\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right)\left(\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\right) &= \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^{-1} \\ &= \begin{pmatrix} a & ac \\ 0 & b \end{pmatrix}\begin{pmatrix} \frac{b}{ab} & 0 \\ 0 & \frac{a}{ab} \end{pmatrix} \\ &= \begin{pmatrix} 1 & \frac{a}{b}c \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

This means that $(a,b) \in F^\times \times F^\times$ acts on $c \in F$ by $(a,b)\cdot c = \frac{a}{b}c$. □

Exercise 5 (Dummit and Foote p. 187 #23)**.** Let K and L be groups, let n be a positive integer, let $\rho : K \to S_n$ be a homomorphism and let H be the direct product of n copies of L. In Exercise 8 of Section 1 an injective homomorphism ψ from S_n into $\mathrm{Aut}(H)$ was constructed by letting the elements of S_n permute the n factors of H. The composition $\psi \circ \rho$ is a homomorphism from G into $\mathrm{Aut}(H)$. The *wreath product* of L by K is the semidirect product $H \rtimes K$ with respect to this homomorphism and is denoted by $L \wr K$ (this wreath product depends on the choice of permutation representation ρ of K—if none is given explicitly, ρ is assumed to be the left regular representation of K).

(a) Assume K and L are finite groups and ρ is the left regular representation for K. Find $|L \wr K|$ in terms of $|K|$ and $|L|$.

(b) Let p be a prime, let $K = L = Z_p$, and let ρ be the left regular representation of K. Prove that $Z_p \wr Z_p$ is a non-abelian group of order p^{p+1} and is isomorphic to a Sylow p-subgroup of S_{p^2}. [The p copies of $\mathbb{Z}_p$ whose direct product makes up H may be represented by p disjoint p-cycles; these are cyclically permuted by K.]

Proof.

(a) By definition, $|L \wr K| = |H \rtimes K|$. Then, by Theorem 10 in Section 5.5, $|H \rtimes K| = |H| \cdot |K|$. Because ρ is the left regular representation for K, the codomain of ρ is $S_{|K|}$. Thus $n = |K|$, and so

$$H = \underbrace{L \times L \times \cdots \times L}_{|K| \text{ times}} = L^{|K|}.$$

Since $|A^m| = |A|^m$ for any set A and any positive integer m, we therefore have

$$|L \wr K| = |L|^{|K|} \cdot |K|,$$

completing the proof of part (a).

(b) By part (a), we have that $|\mathbb{Z}_p \wr \mathbb{Z}_p| = p^p \cdot p = p^{p+1}$, and so $\mathbb{Z}_p \wr \mathbb{Z}_p$ is a group of order p^{p+1}. Furthermore, since $\psi \circ \rho$ is not the trivial homomorphism, Proposition 11 in Section 5.5 implies that K is not a normal subgroup of $H \rtimes_{\psi\circ\rho} K$, and therefore $H \rtimes_{\psi\circ\rho} K$ is not abelian.

Note.

For the sake of clarity, we will use commas to separate the elements of cycles in S_n.

Definition.

1. For $i \in \{1, 2, \ldots, p\}$, let h_i be the cycle in S_{p^2} defined as

$$h_i := \big((i-1)p + 1,\ (i-1)p + 2, \ldots,\ ip\big).$$

2. For $i \in \{1, 2, \ldots, p\}$, let τ_i be the cycle in S_{p^2} defined as

$$\tau_i := (i,\ p + i, \ldots,\ p^2 - p + i).$$

3. Define the element τ of S_{p^2} by

$$\tau := \prod_{i=1}^{p} \tau_i.$$

4. Define the subgroup $\bar{H} \leq S_{p^2}$ as

$$\bar{H} := \langle h_i : i \in \{1, 2, \ldots, p\} \rangle.$$

5. Define the subgroup $\bar{K} \leq S_{p^2}$ as

$$\bar{K} := \langle \tau \rangle.$$

We now prove our first subclaim.

Subclaim 5.1.

$H = \mathbb{Z}_p^p$ is isomorphic to $\bar{H}$.

Proof of subclaim 5.1.

For each $i \in \{1, 2, \ldots, p\}$, let $e_i \in H$ be the element of $\mathbb{Z}_p^p$ with a one in the ith component and zeroes everywhere else. Note that H is generated by $\{e_i : i \in \{1, 2, \ldots, p\}\}$. Let $\varphi_1 : H \to \bar{H}$ be defined over $\{e_i : i \in \{1, 2, \ldots, p\}\}$ as $e_i \mapsto h_i$ and extended "linearly" to H: given any element of H, $v = (v_1, v_2, \ldots, v_p)$ with each $v_i \in \mathbb{Z}_p$ for all $i \in \{1, 2, \ldots, p\}$, define

$$\varphi_1(v) = \prod_{i=1}^{p} h_i^{v_i}.$$

We will show that φ_1 is an isomorphism:

- Homomorphism. Suppose v and w are elements of H. Then we can write

$$v = (v_1, \ldots, v_p), \quad b = (w_1, \ldots, w_p)$$

with $v_i, w_i \in \mathbb{Z}_p$ for each $i \in \{1, \ldots, p\}$. Now we make several notes:

1. For all distinct $i, j \in \{1, \ldots, p\}$, h_i and h_j are disjoint cycles, and therefore $h_i h_j = h_j h_i$.
2. For each $i \in \{1, \ldots, p\}$, the division algorithm guarantees that $v_i + w_i = q_i p + r_i$ for some $r_i \in \{0, \ldots, p-1\} = \mathbb{Z}_p$ and some positive integer q_i.
3. For all $i \in \{1, \ldots, p\}$, h_i is a cycle of length p and thus $h_i^p = (1)$.

We therefore have

$$\begin{aligned}
\varphi_1(v)\varphi_1(w) &= \left[\prod_{i=1}^{p} h_i^{v_i}\right]\left[\prod_{i=1}^{p} h_i^{w_i}\right] \\
&= \prod_{i=1}^{p} h_i^{v_i+w_i} \quad \text{by note 1} \\
&= \prod_{i=1}^{p} h_i^{q_i p + r_i} \quad \text{by note 2} \\
&= \prod_{i=1}^{p} [h_i^{p}]^{q_i} \cdot h_i^{r_i} \\
&= \prod_{i=1}^{p} (1)^{q_i} h_i^{r_i} \quad \text{by note 3} \\
&= \prod_{i=1}^{p} h_i^{r_i} \\
&= \varphi_1(v+w) \quad \text{by note 2.}
\end{aligned}$$

Thus φ_1 is a homomorphism.

- Bijection. Note that φ_1 is surjective onto the generators of $\bar{H}$, $\{h_i : i \in \{1, 2, \ldots, p\}\}$, as h_i is mapped to by e_i for each $i \in \{1, 2, \ldots, p\}$. Then, since this holds for all generators $\bar{H}$, φ_1 is surjective onto all of $\bar{H}$. Furthermore, $|H| = |\bar{H}| = p^p$ obviously, and so every surjection from H to $\bar{H}$ is a bijection. Thus φ_1 is a bijection.

This shows that φ_1 is an isomorphism, proving subclaim 1. □

Note also that $\bar{K}$ is a cyclic group generated by τ which has order p. Thus, by Theorem 4 in Section 2.2, $\varphi_2 : K \to \bar{K}$ defined as $\varphi_2(n) = \tau^n$ is an isomorphism, and hence $K \cong \bar{K}$.

Now we make and prove our second subclaim.

Subclaim 5.2.

Let $\gamma_\tau : \bar{H} \to \bar{H}$ be defined as $\gamma_\tau(h) = \tau h \tau^{-1}$. Then γ_τ is an automorphism.

Proof of subclaim 5.2.

Consider first an arbitrary generator h_i, $i \in \{1, 2, \ldots, p\}$, of $\bar{H}$. Then, by a proposition proved in a lecture,

$$\begin{aligned}
\gamma_\tau(h_i) &= \tau h_i \tau^{-1} \\
&= \tau\big((i-1)p+1,\ (i-1)p+2, \ldots,\ ip\big)\tau^{-1} \\
&= \Big(\tau\big((i-1)p+1\big),\ \tau\big((i-1)p+2\big), \ldots,\ \tau\big(ip\big)\Big).
\end{aligned}$$

One easily verifies that the definition of

$$\tau := \prod_{i=1}^{p} (i,\ p+i, \ldots, p^2 - p + i)$$

implies that $\tau(n) = n + p$, where this is reduced modulo p^2 if necessary. Therefore $\tau h_p \tau^{-1} = (1,\ 2, \ldots,\ p) = h_1$ and, for $i \in \{1, 2, \ldots, p\}$,

$$\tau h_i \tau^{-1} = (ip+1,\ ip+2, \ldots,\ (i+1)p) = h_{i+1}.$$

In other words, reading the indices modulo p, $\gamma_\tau(h_i) = h_{i+1}$.

Now consider an arbitrary element a of $\bar{H}$. Because the generators of $\bar{H}$ commute with one-another, there exist non-negative integers $a_1, \ldots, a_p$ such that

$$a = \prod_{i=1}^{p} h_i^{a_i},$$

and therefore

$$\begin{aligned}\gamma_\tau(a) &= \tau \left(\prod_{i=1}^{p} h_i^{a_i} \right) \tau^{-1} \\ &= \prod_{i=1}^{p} (\tau h_i \tau^{-1})^{a_i} \\ &= \prod_{i=1}^{p} {h_{i+1}}^{a_i}\end{aligned}$$

where again the indices are read modulo p. This proves that $\gamma_\tau(\bar{H}) \subseteq \bar{H}$.

Recall then that γ_τ is a homomorphism. Furthermore, it is surjective onto $\{h_i : i \in \{1, 2, \ldots, p\}\}$, as h_i is mapped to by h_{i-1} (again reading the indices modulo p). Since the h_i's generate $\bar{H}$, then, γ_τ is surjective onto all of $\bar{H}$. Since every surjection from a finite set to itself is a bijection, this implies that γ_τ is an isomorphism from $\bar{H}$ to $\bar{H}$, and hence it is an automorphism. This concludes the proof of subclaim 2.□

Now, since $\bar{K} = \langle \tau \rangle$, we use the result of subclaim 2 to make the following definition:

Definition.

Let $\Gamma : \bar{K} \to \operatorname{Aut}(\bar{H})$ be defined as

$$\Gamma(\tau^n) = \gamma_\tau^n = \gamma_{\tau^n}, \text{ for all integers } n.$$

Note that, since $\bar{K}$ is generated by τ, this defines Γ for every element of $\bar{K}$.

We use this to make and prove our third subclaim.

Subclaim 5.3.

Γ is a homomorphism.

Proof of subclaim 5.3.

Given arbitrary integers n and m,

$$\begin{aligned}\Gamma(\tau^n \cdot \tau^m) &= \Gamma(\tau^{n+m}) \\ &= \gamma_\tau^{n+m} \\ &= \gamma_\tau^n \circ \gamma_\tau^m \\ &= \Gamma(\tau^n) \circ \Gamma(\tau^m).\end{aligned}$$

Since $\bar{K} = \langle \tau \rangle$, this proves that Γ is a homomorphism, completing subclaim 3. $\square$

Because $\Gamma : \bar{K} \to \mathrm{Aut}(\bar{H})$ is a homomorphism by subclaim 5.3, $\bar{H} \rtimes_\Gamma \bar{K}$ is defined. We use this to make and prove the following fourth subclaim:

Subclaim 5.4.

$H \rtimes_{\psi \circ \rho} K$ is isomorphic to $\bar{H} \rtimes_\Gamma \bar{K}$.

Proof of subclaim 5.4.

Let $\Phi : H \rtimes_{\psi orho} K \to \bar{H} \rtimes_\Gamma \bar{K}$ be given by $\Phi\big((h,k)\big) = \big(\varphi_1(h), \varphi_1(k)\big)$ for every $h \in H$, $k \in K$. First note that

$$\begin{aligned}\varphi_1(v + \psi \circ \rho(n)(w)) &= \varphi_1\big((v_1 + w_{1-n}, \ldots, v_p + w_{p-n})\big) \\ &= \prod_{i=1}^{p} h_i^{v_i + w_{i-n}} \\ &= \left(\prod_{i=1}^{p} h_i^{v_i}\right) \cdot \left(\prod_{i=1}^{p} h_i^{w_{i-n}}\right) \\ &= \varphi_1(v) \cdot \prod_{i=1}^{p} h_{i+n}^{w_i} \quad \text{by re-indexing} \\ &= \varphi_1(v) \cdot \prod_{i=1}^{p} (\gamma_{\tau^n}(h_i))^{w_i} \quad \text{by results in subclaim 2} \\ &= \varphi_1(v) \cdot \gamma_{\tau^n}\left(\prod_{i=1}^{p} h_i^{w_i}\right) \\ &= \varphi_1(v) \cdot \Gamma(\tau^n)\big(\varphi_1(w)\big) \\ &= \varphi_1(v) \cdot \Gamma\big(\varphi_2(n)\big)\big(\varphi_1(w)\big),\end{aligned}$$

where the indices are again read modulo p. Therefore

$$\begin{aligned}\Phi\big((v,n)+(w,m)\big) &= \Phi\big((v+\psi\circ\rho(n)(w), n+m)\big)\\ &= \Big(\varphi_1\big(v+\psi\circ\rho(n)(w)\big), \varphi_2(n+m)\Big)\\ &= \Big(\varphi_1(v)\cdot\Gamma(\varphi_2(n))(\varphi_1(w)), \varphi_2(n)\cdot\varphi_2(m)\Big)\\ &= \big(\varphi_1(v),\varphi_2(n)\big)\cdot\big(\varphi_1(w),\varphi_2(m)\big)\\ &= \Phi\big((v,n)\big)\cdot\Phi\big((w,m)\big).\end{aligned}$$

This shows that Φ is a homomorphism. Furthermore, it is a bijection because φ_1 and φ_2 are isomorphisms. This proves that Φ is an isomorphism, completing subclaim 4. □

To end the proof, we make and prove the following fifth subclaim:

Subclaim 5.5.

$\bar{H}\rtimes_\Gamma \bar{K}$ is isomorphic to $\bar{H}\bar{K}$.

Proof of subclaim 5.5.

Let $\delta : \bar{H}\rtimes_\Gamma \bar{K} \to \bar{H}\bar{K}$ be given by $(h,k)\mapsto h\cdot k$. Then we prove several facts about δ:

- Homomorphism. Let $a,b\in\bar{H}$ and $k,\ell\in\bar{K}$ be given arbitrarily. Then, because $\bar{K}=\langle\tau\rangle$, there exist integers n_k and n_ℓ such that $k=\tau^{n_k}$ and $\ell=\tau^{n_\ell}$. Thus

$$\begin{aligned}\Gamma(k)(b)\cdot k &= \Gamma(\tau^{n_k})(b)\cdot k\\ &= \gamma_{\tau^{n_k}}(b)\cdot k\\ &= \big(\tau^{n_k}\cdot b\cdot\tau^{-n_k}\big)\cdot\tau^{n_k}\\ &= \tau^{n_k}\cdot b\\ &= k\cdot b.\end{aligned}$$

  Therefore

$$\begin{aligned}\delta\big((a,k)(b,\ell)\big) &= \delta\big((a\cdot\Gamma(k)(b), k\cdot\ell)\big)\\ &= [a\cdot\Gamma(k)(b)]\cdot[k\cdot\ell]\\ &= a\cdot[\Gamma(k)(b)\cdot k]\cdot\ell\\ &= a\cdot(k\cdot b)\cdot\ell\\ &= \delta\big((a,k)\big)\cdot\delta\big((b,\ell)\big).\end{aligned}$$

  This proves that δ is a homomorphism.

- Injective. Suppose $(h,k)\in\ker(\delta)$. Then $hk=(1)$. This implies that $h=k^{-1}\in\bar{K}$, and thus, under the canonical inclusion of $\bar{H}$ and $\bar{K}$ in $\bar{H}\rtimes_\Gamma\bar{K}$, we have that $(h,e_{\bar{K}})=(e_{\bar{H}},k^{-1})$, and hence $h=e_{\bar{H}}$ and $k=e_{\bar{K}}$. Thus $\ker(\delta)=\{e_{\bar{H}\rtimes_\Gamma\bar{K}}\}$, which, because δ is a homomorphism, implies that δ is injective.

- Surjective. Let $hk \in \bar{H}\bar{K}$ be given arbitrarily. Then $\delta((h,k)) = hk$, and so δ is surjective.

Since δ is therefore a bijective homomorphism, it is an isomorphism by definition, proving subclaim 5.5. $\square$

Combining the results of subclaims 5.4 and 5.5, this yields that $H \rtimes_{\psi \circ \rho} K \cong \bar{H}\bar{K} \leq S_{p^2}$. Since the order of $H \rtimes_{\psi \circ \rho} K$ was shown earlier to be p^{p+1}, and since the exponent of p in the prime factorization of $p^2! = |S_{p^2}|$ is $p+1$, this shows that $H \rtimes_{\psi \circ \rho} K$ is isomorphic to a Sylow p-subgroup of S_{p^2}, proving the result. $\square$

Exercise 6 (Dummit and Foote p. 187 #25)**.** Let $H(\mathbb{F}_p)$ be the Heisenberg group over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (cf. Exercise 20 in Section 4). Prove that $H(\mathbb{F}_2) \cong D_8$, and that $H(\mathbb{F}_p)$ has exponent p and is isomorphic to the first non-abelian group in Example 7.

Proof.

Subclaim 6.1.

$H(\mathbb{F}_2)$ is isomorphic to D_8.

Proof of subclaim 6.1.

Let $R, S \in H(\mathbb{F}_2)$ be defined as

$$R := \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad S := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then

$$\begin{aligned} R^4 &= \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^2 \cdot \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^2 \\ &= \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= I \\ &= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^2 \\ &= S^2. \end{aligned}$$

Furthermore,

$$\begin{aligned} RS &= \begin{pmatrix}1 & 1 & 1\\ 0 & 1 & 1\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} \\ &= \begin{pmatrix}1 & 0 & 1\\ 0 & 1 & 1\\ 0 & 0 & 1\end{pmatrix} \\ &= \begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 1\\ 0 & 0 & 1\end{pmatrix} \\ &= SR^{-1}. \end{aligned}$$

So, since we already have exhibited 5 elements of $H(\mathbb{F}_2)$ that are in $\langle R, S\rangle$ (I, R, S, RS, and R^{-1}), Lagrange's Theorem implies that $H(\mathbb{F}_2) = \langle R, S\rangle$, where $R^4 = S^2 = I$ and $RS = SR^{-1}$. Thus, because D_8 has the defining representation $D_8 = \langle r, s \mid r^4 = s^2 = 1, rs = sr^{-1}\rangle$, the function $\varphi : \{R, S\} \to D_8$ defined by $\varphi(R) = r$ and $\varphi(S) = s$ has a well-defined "linear" extension to all of $H(\mathbb{F}_2)$, and this extension will be a homomorphism by the structural relations we have shown $H(\mathbb{F}_2)$ to have. Additionally, $\psi : D_8 \to H(\mathbb{F}_2)$ defined as $\psi(r) = R$ and $\psi(s) = S$ has a similarly well-defined linear extension, and clearly $\psi \circ \varphi = \varphi \circ \psi = \mathrm{id}$. Thus φ is invertible, and hence φ is an isomorphism from $H(\mathbb{F}_2)$ to D_8, proving the result. □

Subclaim 6.2.

$H(\mathbb{F}_p)$ has exponent p

Proof of subclaim 6.2.

By work done in a previous homework, we found that for all positive integers n,

$$\begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix}^n = \begin{pmatrix}1 & n\cdot a & \frac{1}{2}a\cdot c\cdot n^2 - \frac{1}{2}a\cdot c\cdot n + b\cdot n\\ 0 & 1 & c\cdot n\\ 0 & 0 & 1\end{pmatrix}. \tag{1}$$

Clearly, if $n = p$, the right hand side is the identity matrix, and so the exponent of $H(\mathbb{F}_p)$ is at most p. Furthermore, results from a previous homework showed that $|H(\mathbb{F}_p)| = p^3$, and so Cauchy's Theorem implies that $H(\mathbb{F}_p)$ has an element of order p. This implies that the exponent of p is at least p. Combining these two facts yields that $H(\mathbb{F}_p)$ has exponent p, proving subclaim 6.2. □

We have thus proved 2 of the 3 claims. It remains to be shown that $H(\mathbb{F}_p)$ is isomorphic to the first nonabelian group in Example 7. We begin this journey with a definition.

Definition.

Define A, B, and X in $H(\mathbb{F}_p)$ by

$$A := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B := \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad X := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & p-1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then we make and prove several computational facts, combined into a single subclaim.

Subclaim 6.3.

(i) $A^p = B^p = X^p = I$, where I denotes the 3×3 identity matrix.

(ii) $AB = BA$.

(iii) $XAX^{-1} = AB$.

(iv) $XBX^{-1} = B$.

Proof of subclaim 6.3.

(i) Recall that, as mentioned in Equation 1 in subclaim 6.2,

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \cdot a & \frac{1}{2}a \cdot c \cdot n^2 - \frac{1}{2}a \cdot c \cdot n + b \cdot n \\ 0 & 1 & c \cdot n \\ 0 & 0 & 1 \end{pmatrix} \qquad \forall\, n \in \mathbb{Z}^+.$$

So, when $n = p$, clearly this is the identity matrix. This is in particular true for A, B, and X, proving (i).

(ii) By computation,

$$AB = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = BA.$$

This proves (ii).

(iii) By computation,

$$\begin{aligned} XAX^{-1} &= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & p-1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= AB. \end{aligned}$$

This proves (iii).

(iv) By computation,

$$XBX^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & p-1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & p-1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = B.$$

This proves (iv), completing subclaim 6.3. □

The relations shown in subclaim 6.3 show that, by a similar argument to the proof of subclaim 6.1,

$$\langle A, B, X \rangle \cong \langle a, b, x \mid a^p = b^p = x^p = 1, ab = ba, xax^{-1} = ab, xbx^{-1} = b \rangle$$

which is the first non-abelian group in Example 7. We therefore end by making and proving our final subclaim.

Subclaim 6.4.

$\langle A, B, X \rangle = H(\mathbb{F}_p)$.

Proof of subclaim 6.4.

Note that, for all positive integers n and m, we have by Equation 1 in subclaim 6.2 that

$$A^n B^m = \begin{pmatrix} 1 & n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & m \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n & m \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

So, if $1 \leq n, m \leq p$, then these matrices are distinct: if $A^{n_1} B^{m_1} = A^{n_2} B^{n_2}$ for $1 \leq n_1, m_1, n_2, m_2 \leq p$, then $n_1 = n_2$ and $m_1 = m_2$. Since X is distinct also, we have that $\langle A, B, X \rangle$ contains at least $p^2 + 1$ elements of $H(\mathbb{F}_p)$. Thus, by Lagrange's

Theorem, since $|H(\mathbb{F}_p)| = p^3$, the order of $\langle A, B, X \rangle$ is p^3, and thus $\langle A, B, X \rangle = H(\mathbb{F}_p)$, proving subclaim 6.4. $\square$

Combining subclaim 6.4 with the discussion following subclaim 6.3, we achieve the result. $\square$