Math 120 – Spring 2018 – Prof. Church
Midterm Exam Solutions

Setup: Let p be a prime number. Recall from §1.4 that $\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$ denotes the finite group of invertible $m \times m$ matrices over $\mathbb{Z}/p\mathbb{Z}$ under matrix multiplication:

$$\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z}) = \{\ m \times m \text{ matrices } A \text{ with entries in } \mathbb{Z}/p\mathbb{Z} \ \big|\ \det A \neq 0 \in \mathbb{Z}/p\mathbb{Z}\ \}$$

You may use without proof that $|\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})| = (p^m - 1)(p^m - p)(p^m - p^2)\cdots(p^m - p^{m-1})$.

Say that a matrix $A \in \mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$ is *upper-triangular* if A has 1's on the diagonal and 0's below the diagonal, i.e. if A has the form:

$$A = \begin{bmatrix} 1 & * & * & \cdots & * & * \\ 0 & 1 & * & \cdots & * & * \\ 0 & 0 & 1 & \cdots & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & * \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$$

Let UT_m denote the subgroup consisting of upper-triangular matrices:

$$UT_m = \{A \in \mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z}) \mid A \text{ is upper-triangular}\}$$

You may use without proof that UT_m is a subgroup of $\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$.

Question 1 (15 points)**.** Suppose that G is a finite group. Prove that the following are equivalent:

(A) G is isomorphic to a subgroup of UT_m for some m.

(B) the order of G is a power of p: $|G| = p^k$.

Answer 1. *(A)* $\implies$ *(B)*: we first observe that $|UT_m| = p^{\binom{m}{2}})$. Indeed, for any values in $\mathbb{Z}/p\mathbb{Z}$ in place of the asterisks above, the resulting matrix has determinant 1 and thus belongs to $\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$. For each asterisk, we have p possible values, so $|UT_m| = p^{\#\text{ asterisks}}$. The number of asterisks is $(m-1) + \cdots + 1 = \binom{m}{2}$, so $|UT_m| = p^{\binom{m}{2}}$. If G is isomorphic to a subgroup $H < UT_m$, we know that $|G| = |H|$ and $|H|$ divides $|UT_m|$. Therefore $|G|$ is a power of p.

(B) $\implies$ *(A)*: Lemma 1: Any finite group G is isomorphic to a subgroup of $\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$ for some m.

Proof of Lemma 1: We proved on HW3 Q2 that G is isomorphic to a subgroup of S_n where $n = |G|$. Moreover, considering the $n \times n$ permutation matrices shows that S_n is isomorphic to a subgroup of $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. Together, this shows that G is isomorphic to a subgroup of $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$.

Lemma 2: UT_m is a p-Sylow subgroup of $\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$.

Proof of Lemma 2: The order of $\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$ is

$$\begin{aligned}(p^m-1)(p^m-p)(p^m-p^2)\cdots(p^m-p^{m-1}) &= (p^m-1)p(p^{m-1}-1)p^2(p^{m-2}-1)\cdots p^{m-1}(p-1)\\ &= p^{1+2+\cdots+(m-1)}\prod_{i=1}^{m}(p^i-1)\end{aligned}$$

Since each term of the product $\prod_{i=1}^{m}(p^i-1)$ is -1 mod p, the total product is ±1 mod p. Therefore $p^{1+2+\cdots+(m-1)}=p^{\binom{m}{2}}$ is the largest power of p dividing $|\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})|$. Since UT_m is a subgroup of this size, it is a p-Sylow subgroup.

We now finish the proof that $(B) \implies (A)$. By Lemma 1, G is isomorphic to a subgroup H of $\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$. If G is a p-group, then so is H. So Sylow 2(b) says that H is contained in a p-Sylow P of $\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$. Sylow 1 says that all p-Sylows are conjugate, so there is some $g\in\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$ such that $gPg^{-1}=UT_m$. Then gHg^{-1} is a subgroup of UT_m which is isomorphic to G, as desired.

For Questions 2, 3, and 4, say that two points in $\mathbb{Z}^2$ are *adjacent* if they differ by exactly 1 in exactly one coordinate. In other words, each point $(a, b) \in \mathbb{Z}^2$ is adjacent to exactly four points, namely:

$$\begin{tikzcd}
 & (a, b+1) \arrow[d, dash] & \\
(a-1, b) \arrow[r, dash] & (a, b) \arrow[r, dash] \arrow[d, dash] & (a+1, b) \\
 & (a, b-1) &
\end{tikzcd}$$

Say that a bijection $f \colon \mathbb{Z}^2 \to \mathbb{Z}^2$ is *adjacency-preserving* (for short, that f is an *ap-bijection*) if

$$p \text{ adjacent to } q \qquad \Longleftrightarrow \qquad f(p) \text{ adjacent to } f(q)$$

Let $G = APB(\mathbb{Z}^2)$ be the group of adjacency-preserving bijections $f \colon \mathbb{Z}^2 \to \mathbb{Z}^2$ under composition; you may assume without proof that G is a group.

Question 2 (15 points)**.**
Give a **precise description of all the conjugacy classes** in the group $G = APB(\mathbb{Z}^2)$. Which conjugacy classes contain one element? Which conjugacy classes contain n elements for $n \in \mathbb{N}$? Which (if any) contain infinitely many elements? Justify your answers. Possible hint: start by figuring out a good way to list/label all the elements of G.

Answer 2. We first note two convenient subgroups of G. First, for $(a, b) \in \mathbb{Z}^2$, let $t_{a,b}$ be the translation $(x, y) \mapsto (x + a, y + b)$. These translations together form a subgroup T isomorphic to $\mathbb{Z}^2$. Second, let r be the 90-degree rotation sending $(x, y) \mapsto (y, -x)$ and let s be the reflection $(x, y) \mapsto (x, -y)$. The 8 elements $\{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$ form a subgroup D isomorphic to D_8. (We will see later that this subgroup is the stabilizer of the origin.) An alternate way to describe this subgroup is as the union of the 4 elements sending (x, y) to $(\pm x, \pm y)$ [with the 4 elements corresponding to the 4 choices of $+$ or $-$] with the 4 elements sending (x, y) to $(\pm y, \pm x)$. We claim that $G \cong T \rtimes D$; we will prove this over the course of the next three lemmas.

Lemma 2.1. *Every $g \in G$ can be uniquely written as $td = t_{a,b}r^is^j$ for some $t = t_{a,b} \in T$ and some $d = r^is^j \in D$.*

Proof. Note that once we prove existence, uniqueness is easy: if $g = t_{a,b}d = t_{a',b'}d'$ then we have $g(0, 0) = t_{a,b}(0, 0) = (a, b)$ but also $g(0, 0) = t_{a',b'}(0, 0) = (a', b')$. Therefore $(a', b') = (a, b)$. Left-multiplying by $t^{-1}_{a,b}$ then shows $d = d'$ as well.

Consider an ap-bijection g, and suppose that $g(0, 0) = (a, b)$. Let $h = t^{-1}_{(a,b)}g$. Note that $h(0, 0) = t^{-1}_{(a,b)}(a, b) = (0, 0)$.

Since h is adjacency-preserving, it must take $(1, 0)$ to either $(1, 0)$, $(0, 1)$, $(-1, 0)$, or $(0, -1)$. Let $k = r^{-i}h$ where $i = 0, 1, 2,$ or 3 respectively. This choice guarantees that $k(1, 0) = (1, 0)$, and still $k(0, 0) = (0, 0)$.

Since k is adjacency-preserving, it must take $(0,1)$ to either $(0,1)$, $(-1,0)$, or $(0,-1)$. Moreover the middle option cannot actually happen: since $(0,1)$ shares *two* neighbors with $(1,0)$, it must be taken to some point that shares two neighbors with $(1,0)$. Therefore $k(0,1)$ is either $(0,1)$ or $(0,-1)$. Let $f = s^{-j}k$ where $j = 0$ or 1 respectively.

We now have that f is an adjacency-preserving bijection fixing $(0,0)$, $(1,0)$, and $(0,1)$, and $g = t_{a,b}r^i s^j f$. Therefore to finish the proof of Lemma 1, it suffices to prove the following lemma: □

Lemma 2.2. The only adjacency-preserving bijection f fixing $(0,0)$, $(1,0)$, and $(0,1)$ is the identity.

Proof. We prove by a sort of induction that such an f fixes every point in $\mathbb{Z}^2$. First, note that $f(2,0)$ must be a neighbor of $f(1,0) = (1,0)$ that shares no neighbors with $f(0,0) = (0,0)$, so $f(2,0)$ must be $(2,0)$. By induction, we conclude that f fixes all points on the x-axis.

Abstracting this argument, what it really shows is that whenever an ap-bijection fixes two adjacent points, it fixes the entire (vertical or horizontal) line through those points. For example, applying the same argument to $(0,0)$ and $(0,1)$ shows that f fixes all points on the y axis. But then e.g. $(1,1)$ must be sent to a point adjacent to both $(0,1)$ and $(1,0)$, and the origin is already fixed, so the only option is $(1,1)$ itself. Now that $(1,1)$ is fixed, applying the argument to $(0,1)$ and $(1,1)$ shows that the entire line $y = 1$ must be fixed. Finally, applying the argument to $(k,0)$ and $(k,1)$ shows that the entire line $x = k$ must be fixed for any k. Therefore f is the identity. □

Lemma 2.3. *T is a normal subgroup of G.*

Proof. Suppose $t = t_{a,b}$ and $g = t_{x,y}d$. Then $g^{-1}tg = d^{-1}t_{x,y}^{-1}t_{a,b}t_{x,y}d = d^{-1}t_{a,b}d$ since T is abelian. Therefore it suffices to check that $dTd^{-1} = T$ for each of the 8 elements of D. Since D is generated by r and s, it suffices to check that $rTr^{-1} = T$ and $sTs^{-1} = T$. Direct computation shows that $rt_{a,b}r^{-1} = t_{b,-a}$ and $st_{a,b}s^{-1} = t_{a,-b}$, verifying the desired claim (and also used later). □

Lemma 2.1 showed that $G = TD$ and Lemma 2.3 shows that $T \triangleleft G$, and it is clear that $T \cap D = \{1\}$. Therefore $G \cong T \rtimes D$. (This is not necessary yet, but we will use it later.) The action of D on T by conjugation is as follows: if $d(x,y) = (\pm x, \pm' y)$, then $d = d^{-1}$ and $dt_{a,b}d^{-1} = t_{\pm a, \pm' b}$; if $d(x,y) = (\pm y, \pm' x)$ then $d^{-1}(x,y) = (\pm' y, \pm x)$ and thus $dt_{a,b}d^{-1} = t_{\pm b, \pm' a}$.

We are now ready to describe the conjugacy classes:

The conjugacy class of $t_{a,b}$ consists of the elements $t_{\pm a, \pm b}$ and the elements $t_{\pm b, \pm a}$. Indeed, we saw in the proof of Lemma 2.3 that the conjugates of $t_{a,b}$ by all of G are the same as the conjugates $dt_{a,b}d^{-1}$ for $d \in D$, which are precisely the elements listed. These are 8 potential elements, but there can be duplicates. This conjugacy class has size 8 if $|a|$ and $|b|$ are nonzero and different; size 4 if exactly one is zero or if $|a| = |b| \neq 0$; and size 1 if $|a| = |b| = 0$.

For elements of the form $t_{a,b}d$ with $d \neq 1$, there is a different behavior. Note that since T is normal, the assignment $td \mapsto d$ is a homomorphism $G \twoheadrightarrow D_8$. Therefore elements can only be conjugate if their d factors are conjugate in D_8. Those conjugacy classes are: (A) rotation by 180 degrees ($\{r^2\}$); (B) rotation by 90 and by 270 degrees ($\{r, r^3\}$); (C) vertical and horizonal reflection ($\{s, r^2 s\}$); and (D) the two diagonal reflections ($\{rs, r^3 s\}$).

These split into conjugacy classes as (proofs below); each of these conjugacy classes is infinite:

(A1) $\{t_{a,b}r^2 \,|\, a \equiv b \equiv 0 \bmod 2\}$

(A2) $\{t_{a,b}r^2 \,|\, a \equiv b \equiv 1 \bmod 2\}$

(A3) $\{t_{a,b}r^2 \,|\, a \not\equiv b \bmod 2\}$

(B1) $\{t_{a,b}r^{\pm 1} \,|\, a \equiv b \bmod 2\}$

(B2) $\{t_{a,b}r^{\pm 1} \,|\, a \not\equiv b \bmod 2\}$

(C1$_n$) $\{t_{a,b}s \,\big|\, |a| = n, b \equiv 0 \bmod 2\} \cup \{t_{a,b}r^2 s \,\big|\, |b| = n, a \equiv 0 \bmod 2\}$

(C2$_n$) $\{t_{a,b}s \,\big|\, |a| = n, b \equiv 1 \bmod 2\} \cup \{t_{a,b}r^2 s \,\big|\, |b| = n, a \equiv 1 \bmod 2\}$

(D1$_n$) $\{t_{a,b}rs \,\big|\, |a+b| = n, a \equiv b \bmod 2\} \cup \{t_{a,b}r^3 s \,\big|\, |a-b| = n, a \equiv b \bmod 2\}$

(D2$_n$) $\{t_{a,b}rs \,\big|\, |a+b| = n, a \not\equiv b \bmod 2\} \cup \{t_{a,b}r^3 s \,\big|\, |a-b| = n, a \not\equiv b \bmod 2\}$

For purposes of showing that two elements *can't* be conjugate, we note the following lemma (ok to omit proof here): if $t_{a,b}d$ is conjugate to $t_{a',b'}d'$, then $a + b \equiv a' + b' \bmod 2$. Another way to say this is that $a \equiv b \bmod 2 \iff a' \equiv b \bmod 2$. This shows, for example, that (B1) and (B2) must be two different conjugacy classes. It also shows that (D1$_n$) cannot be conjugate to (D2$_m$).

(A): suppose $g = t_{a,b}r^2$ and $h = t_{p,q}d$. Then

$$\begin{aligned} hgh^{-1} &= t_{p,q}dt_{a,b}r^2d^{-1}t_{p,q}^{-1} \\ &= t_{p,q}(dt_{a,b}d^{-1})r^2t_{-p,-q} \\ &= t_{p,q}(dt_{a,b}d^{-1})t_{p,q}r^2 \\ &= \begin{cases} t_{2p\pm a,2q\pm' b}r^2 & \text{if } d(x,y) = (\pm x, \pm' y) \\ t_{2p\pm b,2q\pm' a}r^2 & \text{if } d(x,y) = (\pm y, \pm' x) \end{cases} \end{aligned}$$

Therefore we see that the conjugacy class of $g = t_{a,b}r^2$ consists of exactly those elements $k = t_{z,w}r^2$ with either $z \equiv a \bmod 2$ and $w \equiv b \bmod 2$, or $z \equiv b \bmod 2$ and $w \equiv a \bmod 2$. Therefore the elements of the form tr^2 split up into three infinite conjugacy classes: (A1) where $a \equiv b \equiv 0 \bmod 2$, (A2) where $a \equiv b \equiv 1 \bmod 2$, and (A3) where $a \not\equiv b \bmod 2$). For what it's worth, each of the elements of the form tr^2 is the inversion through a point in the plane — and these three conjugacy classes correspond to whether that point has integer coordinates (A1); half-integer coordinates (A2); or one integer coordinate and one half-integer coordinate (A3).

(B): We noted above that elements (B1) cannot be conjugate to elements (B2). So it suffices to check that everything in B1 is conjugate, and similarly for B2. We start with B1.

First, note that r is conjugate to r^3 (by s). Next, note that

$$t_{x,y}rt_{x,y}^{-1} = t_{x,y}rt_{-x,-y} = t_{x,y}t_{y,-x}r = t_{y+x,y-x}r.$$

For any a, b with $a \equiv b \bmod 2$, the system of equations $y + x = a$, $y - x = b$ is uniquely solvable in integers; therefore for any such a, b we have $t_{x,y} r t_{x,y}^{-1} = t_{a,b} r$. Similarly, for r^3 we have

$$t_{x,y} r^3 t_{x,y}^{-1} = t_{x,y} r^3 t_{-x,-y} = t_{x,y} t_{-y,x} r^3 = t_{x-y,x+y} r^3.$$

Again this is solvable when $a \equiv b \bmod 2$, so r^3 is conjugate to $t_{a,b} r^3$. This concludes the proof that everything in (B1) is conjugate. The proof for (B2) is pretty much identical, except we start by showing that $t_{1,0} r$ is conjugate to $t_{1,0} r^3$ (by s).

(C): These elements fall into two infinite families of conjugacy classes, (C1$_n$) for $n \geq 0$ and (C2$_n$) for $n \geq 0$. Each of these conjugacy classes is infinite. To see that they are distinct, one way to argue is as follows. For an element g, let $\ell(g)$ be the minimum distance (in the Manhattan metric) between $p \in \mathbb{Z}^2$ and $g(p) \in \mathbb{Z}^2$:

$$\ell(g) = \min_{p \in \mathbb{Z}^2} \operatorname{dist}(p, g \cdot p).$$

Let minset(g) denote the set of $p \in \mathbb{Z}^2$ which realize this minimum:

$$\operatorname{minset}(g) = \operatorname{argmin}_{p \in \mathbb{Z}^2} \operatorname{dist}(p, g \cdot p).$$

We introduce these invariants because $\ell(hgh^{-1}) = \ell(g)$ and $\operatorname{minset}(hgh^{-1}) = h \cdot \operatorname{minset}(g)$; so if two elements have different ℓ or non-equivalent minset, they cannot be conjugate.

For $g = t_{a,b} s$ in $(C1_n)$, we have $\ell(g) = |a| = n$ and minset(g) is a single horizontal line $y = b/2$ (g is a translation-plus-reflection along this line). Similarly, for $g = t_{a,b} r^2 s$ in $(C1_n)$ we have $\ell(g) = |b| = n$ and minset(g) is a single vertical line $x = a/2$.

For $g = t_{a,b} s$ in $(C2_n)$, we have $\ell(g) = |a| + 1 = n + 1$ and minset(g) is *two* adjacent lines $y = \lfloor b/2 \rfloor$ and $y = \lceil b/2 \rceil$ (g is a translation-plus-reflection along the line $y = b/2$ midway between them). Similarly for $g = t_{a,b} r^2 s$ in $(C2_n)$, we have $\ell(g) = |b| + 1 = n + 1$ and minset(g) is two adjacent vertical lines $x = \lfloor a/2 \rfloor$ and $y = \lceil a/2 \rceil$.

It remains to show that for fixed n, every element of $(C1_n)$ is conjugate, and similarly for $(C2_n)$.

We first note that $t_{-n,b} s$ is conjugate to $t_{n,b} s$ (by $r^2 s$), and similarly $t_{a,-n} r^2 s$ is conjugate to $t_{a,n} r^2 s$ (by s). Next, note that $t_{n,b} s$ is conjugate to $t_{n,b+2} s$ (by $t_{p,1}$), and similarly $t_{a,n} r^2 s$ is conjugate to $t_{a+2,n} r^2 s$ (by $t_{1,q}$). This already shows that the left side of $(C1_n)$ is all conjugate, as is the right side; and similarly that the left side of $(C2_n)$ is all conjugate, as is the right side. Finally, we note that $t_{n,0} s$ is conjugate to $t_{0,n} r^2 s$ (by r), and similarly $t_{n,1} s$ is conjugate to $t_{-1,n} r^2 s$ (by r). This concludes the proof that $(C1_n)$ forms a single conjugacy class, and similarly for $(C2_n)$.

(D): This proof is very similar to the argument for (C). We have already noted that (D1$_n$) cannot be conjugate to (D2$_m$). To show that D1$_n$ cannot be conjugate to D1$_m$ for $m \neq n$, we could copy the argument for (C), but for variety we phrase it differently. Note that if g is conjugate to k then g^2 is conjugate to k^2. If $g = t_{a,b} rs$ then $g^2 = t_{a+b,a+b}$; similarly if $g = t_{a,b} r^3 s$ then $g^2 = t_{a-b,b-a}$. But we know from the discussion of elements of T that $t_{n,n}$ is only conjugate to $t_{n,-n}$, $t_{-n,n}$, and $t_{-n,-n}$. This shows that the number n is an invariant of the conjugacy class.

It remains to show that everything in (D1$_n$) is conjugate, and everything in (D2$_n$) is conjugate. This works just the same as for (C) — for example, $t_{a,b} rs$ is conjugate to $t_{0,a+b} rs$ (by $t_{0,a}$) — so we omit the details.

Question 3 (20 points)**.**
This question has 4 parts, each worth 5 points. For each of the following, either give an example of the normal subgroup N_k or prove that no such normal subgroup exists. (When giving examples, as long as your example is correct, you do not have to *prove* that it is a normal subgroup; however it might be safer to sketch the proof, so you can still get partial credit if there's a mistake.)

(a) Does G have a normal subgroup N_2 of index $[G : N] = 2$?

Answer 3(a). Yes. If $H \lhd D$ is a normal subgroup of index k, then $N = T \rtimes H$ will be a normal subgroup of $T \rtimes D$ of index k. For 3(a) we can take any normal index-2 subgroup of D, for example $\{1, r, r^2, r^3\}$. The resulting index-2 subgroup of G consists of elements tr^i, which are precisely the "orientation-preserving" maps (if we wanted to go to the trouble of formalizing what that means). You could also take one of the other two normal index-2 subgroups $H \lhd D$.

The one essentially different index-2 normal subgroup is $N = \{t_{a,b}d \,|\, a \equiv b \bmod 2\}$. To show that this is a subgroup, note that $(t_{a,b}d)(t_{p,q}d') = (t_{a,b}(dt_{p,q}d^{-1})dd'$. So one needs only to show that the condition $p \equiv q \bmod 2$ is preserved by $(p, q) \mapsto d(p, q)$. But we know that $d(p, q) = (\pm p, \pm' q)$ or $(\pm q, \pm' p)$, so this is indeed true.

[Of course, you were only asked to find one example, not classify all the possibilities — this is just a remark by me.]

(b) Does G have a normal subgroup N_4 of index $[G : N] = 4$?

Answer 3(b). One possibility is to take $T \rtimes H$ where H is a normal index-4 subgroup of D. The only choice here is $H = \{1, r^2\}$, so $N = \{t_{a,b}r^2\} \cup \{t_{a,b}r^2\}$. Another option is, inside of $G \cong \mathbb{Z}^2 \rtimes D$, to take the normal subgroup $N = (2\mathbb{Z})^2 \rtimes D$, i.e. $N = \{t_{2a,2b}d\}$.

(c) Does G have a normal subgroup N_5 of index $[G : N] = 5$?

Answer 3(c). No. There are many ways to do it. Here is one rather lazy argument: if N_5 was a normal subgroup of index 5, then $H = G/N_5$ would be a group of order 5. Since 5 is prime, H must be cyclic; in particular, H is abelian. But there is a surjective homomorphism $G \twoheadrightarrow G/N_5$ so Question 4 implies that $|H|$ divides 8. Since 5 does not divide 8, this is a contradiction.

(d) Does G have a normal subgroup N_{72} of index $[G : N] = 72 = 8 \cdot 9 = 2^3 \cdot 3^2$?

Answer 3(d). Yes. One choice (by far the most natural) is $\big((3\mathbb{Z})^2 \rtimes 1\big) \lhd \big(\mathbb{Z}^2 \rtimes D\big) \cong G$, i.e. $N_{72} = \{t_{3a,3b}\}$. Another possibility is $\big((6\mathbb{Z})^2 \rtimes H\big) \lhd \big(\mathbb{Z}^2 \rtimes D\big)$ where $H \lhd D$ has $|H| = 4$, e.g. $N_{72} = \{t_{6a,6b}r^i\}$.

Question 4 (15 points)**.**
Suppose that $G \twoheadrightarrow H$ is a surjective homomorphism, and H is an abelian group.
Prove that $|H|$ is finite and $|H|$ divides 8.

Answer 4. Let N be the commutator subgroup of G, and let $K = \ker(G \to H)$.

Lemma 4.1. If H is abelian, then $N \subset K$.

Proof. Write $[a, b]$ for the commutator $[a, b] = a^{-1}b^{-1}ab$. Since H is abelian, we have

$$f([a,b]) = f(a^{-1}b^{-1}ab) = f(a)^{-1}f(b)^{-1}f(a)f(b) = f(a)^{-1}f(a)f(b)^{-1}f(b) = 1.$$

So every commutator is contained in K. Since N is generated by commutators, we conclude that $N \subset K$. □

By one of the isomorphism theorems, $H \cong G/K$ is isomorphic to $(G/N)/(K/N)$. The point is that H is a quotient of G/N. Therefore it suffices to prove that G/N has order 8 (or just dividing 8, although actually it does have order 8).

We begin by simply listing certain elements that are commutators, and thus belong to N.

$$\begin{aligned}
[r^2, t_{1,0}] &= t_{2,0} \in N \\
[r^2, t_{0,1}] &= t_{0,2} \in N \\
[rs, t_{1,0}] &= t_{1,1} \in N \\
[s, r] &= r^2 \in N
\end{aligned}$$

Note that the first three generate the subgroup $\{t_{a,b} \mid a \equiv b \bmod 2\}$ (which has index 2 in T).

This will be enough for us to show that N has at most 8 cosets. These 8 cosets (which we do not need to prove are distinct, although they are) are represented by:

$$\text{the 8 elements } td \text{ for } t \in \{t_{0,0}, t_{1,0}\} \text{ and } d \in \{1, r, s, sr\} \qquad (*)$$

. We will show that every element in G is congruent mod N to one of these 8 elements $(*)$.

Suppose that $g = t_{a,b}r^is^j$. If $a \equiv b \bmod 2$, then $t_{a,b} \in N$, so $g \equiv r^is^j$. If not, then $t_{a-1,b} \in N$, so $g \equiv t_{1,0}r^is^j$. Moreover, since $r^2 \in N$ we can replace r^2 by r^0 or replace r^3 by r. This shows that every $g = t_{a,b}r^is^j$ is equivalent to

$$[t_{0,0} \text{ or } t_{1,0}][r^0 \text{ or } r^1][s^0 \text{ or } s^1].$$

This shows that $|G/N| \leq 8$.

This is not quite enough, since we were asked to show that $|H|$ *divides* 8. But we can use the rewriting rules above to check that each of the 8 representatives h in $(*)$ has order 2 mod N, i.e. $h^2 \in N$. (For example, $r^2 \in N$; $(t_{1,0}s)^2 = t_{2,0} \in N$, and so on.) This implies that every element of G/N has order 2 (or 1). So by Cauchy's theorem $|G/N|$ cannot have any other prime factors. Therefore although we have technically left open the possibility that $|G/N|$ could be less than 8, it must be a power of 2, which suffices for the problem.

Question 5 (35 points)**.** This question has 7 parts, each worth 5 points. In your solution to one part, you **may assume the results of all preceding parts**, whether or not you solved those earlier parts. For example, in your solution to (f) you may assume that $|N| = 56$ since this is the result of (e), even if you have not solved (e).

Let A be the abelian group $A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = (\mathbb{Z}/2\mathbb{Z})^3$, which has order 8. Let $G = \operatorname{Aut}(A)$ be the group of automorphisms of A. Its order is $|G| = 168 = 2^3 \cdot 3 \cdot 7$.

(You may assume this without proof.)

In this problem, you will prove that G is a *simple group*: it contains no normal subgroups other than $\{1\}$ and G itself. Therefore assume that $N \lhd G$ is a normal subgroup of G, and that $\{1\} \neq N \neq G$. We will eventually prove that this leads to a contradiction.

(a) Let v be the nonzero vector $v = (1, 0, 0) \in A$, and let $H = \operatorname{Stab}_G(v)$ be its stabilizer. Prove that N is not contained in H.

(Hint: otherwise, show that N would be contained in all the conjugates of H.)

(b) Prove that N contains an element of order 7.

(c) Prove that there is more than one 7-Sylow subgroup of G.

(One possible route: show that $f(a, b, c) = (c, a + c, b)$ and $g(a, b, c) = (b, c, a + b)$ define two order-7 elements $f \in G$ and $g \in G$ that do not commute. There are other approaches as well.)

(d) Show that G contains exactly 48 elements of order 7.

(e) Prove that all 48 elements of G of order 7 are contained in N, and conclude that $|N| = 56$.

(f) Let K be the subgroup of G consisting of automorphisms that permute the three elements $(1, 0, 0)$, $(0, 1, 0)$, and $(0, 0, 1)$ of A. There is an isomorphism $\psi \colon S_3 \xrightarrow{\cong} K$.

(You may use this without proof.)

Prove that K is contained in N.

(g) Obtain a contradiction from the preceding parts.

(a) Let v be the nonzero vector $v = (1, 0, 0) \in A$, and let $H = \mathrm{Stab}_G(v)$ be its stabilizer. Prove that N is not contained in H.

(Hint: otherwise, show that N would be contained in all the conjugates of H.)

Answer 5(a). Suppose for a contradiction that $N \subseteq H$. This would imply $N = gNg^{-1} \subseteq gHg^{-1}$. Therefore $N \subseteq \bigcap_{g\in G} gHg^{-1}$. To obtain a contradiction, we prove that $\bigcap_{g\in G} gHg^{-1} = \{1\}$.

Lemma 5.1. For any group action, if $H = \mathrm{Stab}_G(v)$, then $gHg^{-1} = \mathrm{Stab}_G(g \cdot v)$.

Proof. I would probably accept this without a proof, but here's one anyway: $ghg^{-1} \cdot (g \cdot v) = gh \cdot v = g \cdot v$, which shows that $gHg^{-1} \subseteq \mathrm{Stab}_G(g \cdot v)$. Conversely, if $k \in \mathrm{Stab}_G(g \cdot v)$ then $g^{-1}kg \cdot v = g^{-1} \cdot gv = v$, so $g^{-1}kg \in H$, i.e. $\mathrm{Stab}_G(g \cdot v) \subseteq gHg^{-1}$. □

Therefore $\bigcap_{g\in G} gHg^{-1} = \bigcap_{g\in G} \mathrm{Stab}_G(g \cdot v)$. Suppose that α belongs to this intersection; in other words, α fixes $g \cdot v$ for all g. But I claim that every nonzero element of A can be written as $g \cdot v$ for some g (indeed we will see explicit elements below). Therefore our assumption implies that α fixes each of the seven nonzero elements of A. Since the identity element is always preserved by any automorphism, we conclude that α is the identity, as claimed.

Recall:	$A = (\mathbb{Z}/2\mathbb{Z})^3$	$G = \mathrm{Aut}(A)$	$\lvert G\rvert = 168 = 2^3 \cdot 3 \cdot 7$
	$v = (1, 0, 0)$	$H = \mathrm{Stab}_G(v)$	
	$N \lhd G$	$\{1\} \neq N \neq G$	

(b) Prove that N contains an element of order 7.

Answer 5(b). We saw above that the orbit of v under G is all seven nonzero elements of A. By the orbit-stabilizer theorem, the order of H is $|G|/7 = 2^3 \cdot 3 = 24$.

Since N is normal, we know that NH is a subgroup. Its order is $|NH| = \frac{|N|\cdot|H|}{|N \cap H|}$. We can rewrite this as $|NH| = |H| \cdot [N : N \cap H]$. Since N is not contained in H by (a), we know that the index $[N : N \cap H]$ must be bigger than 1. Therefore $|NH|$ is a proper multiple of $2^3 \cdot 3$ which still divides $|G| = 2^3 \cdot 3 \cdot 7$. The only way this is possible is if $NH = G$, and the index $[N : N \cap H] = 7$.

In particular, this implies that $|N|$ is divisible by 7. By Cauchy's theorem, N contains an element of order 7.

Recall:	$A = (\mathbb{Z}/2\mathbb{Z})^3$	$G = \mathrm{Aut}(A)$	$|G| = 168 = 2^3 \cdot 3 \cdot 7$
	$v = (1,0,0)$	$H = \mathrm{Stab}_G(v)$	
	$N \triangleleft G$	$\{1\} \neq N \neq G$	
	(a) N is not contained in H		

(c) Prove that there is more than one 7-Sylow subgroup of G.

(One possible route: show that $f(a,b,c) = (c, a+c, b)$ and $g(a,b,c) = (b, c, a+b)$ define two order-7 elements $f \in G$ and $g \in G$ that do not commute. There are other approaches as well.)

Answer 5(c). We first show that $f(a,b,c) = (c, a+c, b)$ is an element of order 7. Its powers are:

$$\begin{aligned}
f^1(a,b,c) &= (c, a+c, b) \\
f^2(a,b,c) &= (b, b+c, a+c) \\
f^3(a,b,c) &= (a+c, a+b+c, b+c) \\
f^4(a,b,c) &= (b+c, a+b, a+b+c) \\
f^5(a,b,c) &= (a+b+c, a, a+b) \\
f^6(a,b,c) &= (a+b, c, a) \\
f^7(a,b,c) &= (a, b, c)
\end{aligned}$$

Therefore $P = \langle f \rangle$ is a 7-Sylow subgroup. If there was only one 7-Sylow subgroup, it would be normal. In particular, gfg^{-1} would be in $\langle f \rangle$ for all g. But choosing $g(a,b,c) = (b,a,c)$ we have

$$gfg^{-1}(a,b,c) = gf(b,a,c) = g(c, b+c, a) = (b+c, c, a$$

Since this does not appear in the list above, we see that $gfg^{-1} \notin P$, so P is not normal.

Recall: $A = (\mathbb{Z}/2\mathbb{Z})^3$ $\quad G = \mathrm{Aut}(A)$ $\quad |G| = 168 = 2^3 \cdot 3 \cdot 7$

$v = (1,0,0)$ $\quad H = \mathrm{Stab}_G(v)$

$N \triangleleft G$ $\quad \{1\} \neq N \neq G$

(a) N is not contained in H

(b) N contains an element of order 7

(d) Show that G contains exactly 48 elements of order 7.

Answer 5(d). By Sylow we know that $n_7(G) \equiv 1 \bmod 7$ and $n_7(G)$ divides 24. The only possibilities are $n_7(G) = 1$ and $n_7(G) = 8$. We just proved in (c) that $n_7(G) \neq 1$, so $n_7(G) = 8$. Therefore there are exactly 8 Sylow 7-subgroups, each containing 6 elements of order 7. Since these have prime order, distinct 7-Sylows must be disjoint except for the identity. Therefore there are exactly $6 \cdot 8 = 48$ elements of order 7 lying in some 7-Sylow. By Sylow 2(b), every element of order 7 is contained in some 7-Sylow, so this is all the elements of order 7.

Recall:	$A = (\mathbb{Z}/2\mathbb{Z})^3$	$G = \mathrm{Aut}(A)$	$\lvert G\rvert = 168 = 2^3 \cdot 3 \cdot 7$
	$v = (1, 0, 0)$	$H = \mathrm{Stab}_G(v)$	
	$N \lhd G$	$\{1\} \neq N \neq G$	
	(a) N is not contained in H		
	(b) N contains an element of order 7		
	(c) $n_7(G) > 1$		

(e) Prove that all 48 elements of G of order 7 are contained in N, and conclude that $|N| = 56$.

Answer 5(e). We know from (b) that N contains an element of order 7. Let P be the subgroup of order 7 that it generates. P is a 7-Sylow of G. By Sylow 2(a), all 7-Sylows of G are conjugate. Therefore every element of order 7 belongs to gPg^{-1} for some $g \in G$. However since N is normal, $P \subseteq N$ implies $gPg^{-1} \subseteq gNg^{-1} = N$. Therefore all 48 elements of order 7 are contained in N.

In particular, this tells us that $n_7(N)$ is also 8. Recall that if $|N| = 7 \cdot \ell$ then $n_7(N)$ divides ℓ. Since ℓ must be a proper divisor of 24 (otherwise $|N|$ would be all of $|G|$), this implies that $|N| = 7 \cdot 8 = 56$.

Recall: $A = (\mathbb{Z}/2\mathbb{Z})^3$ $\quad$ $G = \mathrm{Aut}(A)$ $\quad$ $|G| = 168 = 2^3 \cdot 3 \cdot 7$

$v = (1, 0, 0)$ $\quad$ $H = \mathrm{Stab}_G(v)$

$N \lhd G$ $\quad$ $\{1\} \neq N \neq G$

(a) N is not contained in H $\quad$ (d) G contains 48 elements of order 7

(b) N contains an element of order 7

(c) $n_7(G) > 1$

(f) Let K be the subgroup of G consisting of automorphisms that permute the three elements $(1,0,0)$, $(0,1,0)$, and $(0,0,1)$ of A. There is an isomorphism $\psi\colon S_3 \xrightarrow{\cong} K$.

(You may use this without proof.)

Prove that K is contained in N.

Answer 5(f). Consider the quotient group G/N. Since $|N| = 56$ we know that $|G/N| = |G| \,/\, |N| = 168/56 = 3$. Therefore $G/N \cong Z_3$. Let $\pi\colon G \twoheadrightarrow G/N \cong Z_3$ be the quotient map.

Consider the restriction $p = \pi|_K\colon K \to Z_3$. I claim p is the trivial homomorphism. Indeed, since $(i\ j) \in S_3$ has order 2, and Z_3 contains no elements of order 2, $p(i\ j)$ must be the identity. But we proved on HW3 Q1 that the transpositions genereate S_3, so it follows that $p(\sigma)$ is the identity for all $\sigma \in S_3$. In other words, this means that every $k \in K$ actually belongs to N, as desired.

Recall: $A = (\mathbb{Z}/2\mathbb{Z})^3$ $\quad G = \mathrm{Aut}(A)$ $\quad |G| = 168 = 2^3 \cdot 3 \cdot 7$

$v = (1,0,0)$ $\quad H = \mathrm{Stab}_G(v)$

$N \lhd G$ $\quad \{1\} \neq N \neq G$

(a) N is not contained in H $\quad$ (d) G contains 48 elements of order 7

(b) N contains an element of order 7 $\quad$ (e) N contains 48 elements of order 7

(c) $n_7(G) > 1$ $\quad$ (e) $|N| = 56$

(g) Obtain a contradiction from the preceding parts.

Answer 5(g). We showed in (f) that K is a subgroup of N. But $|K| = 6$ and we showed in (e) that $|N| = 56$. Since 6 does not divide 56, this is a contradiction.

Recall:

$A = (\mathbb{Z}/2\mathbb{Z})^3$ $\quad$ $G = \mathrm{Aut}(A)$ $\quad$ $|G| = 168 = 2^3 \cdot 3 \cdot 7$

$v = (1, 0, 0)$ $\quad$ $H = \mathrm{Stab}_G(v)$

$N \lhd G$ $\quad$ $\{1\} \neq N \neq G$

(a) N is not contained in H

(b) N contains an element of order 7

(c) $n_7(G) > 1$

(d) G contains 48 elements of order 7

(e) N contains 48 elements of order 7

(e) $|N| = 56$

(f) the subgroup $K \cong S_3$ is contained in N