

Question 1

First we will find the order of this group. We see that if we consider all 2×2 matrices over \mathbb{Z}_3 , then that is 3^4 possible elements. Since this is $GL_2(\mathbb{Z}_3)$, we know to expect less elements, since we require they be invertible. We recognize invertability can be found with the determinant, and that the determinant is zero only if we have pairing of elements. That is, suppose

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad a, b, c, d \in \mathbb{Z}_3.$$

Then, we know that $\det(A) = ad - bc = 0 \iff a = c \& b = d$ or $a = b \& c = d$, which is $4 \times 3^2 - 3$ elements (where the 4 comes from overlap of the three matrices with all elements the same). Then,

$$|GL_2(\mathbb{Z}_3)| = 3^4 - 4 \cdot 3^2 + 3 = 48 = 6 \cdot 8 = 3 \cdot 2^4.$$

By the first Sylow theorem, we see that the size of the Sylow 3-subgroups is just 3. By the third Sylow theorem, we know

$$n_3 \equiv 1 \pmod{3} \quad \& \quad n_3 | 2^4 = 16.$$

So, our candidates for n_3 are 1, 4 and 16. To actually find the subgroups, we only need find one and then apply the second Sylow theorem, since the rest better be conjugates of the one we find. From inspection, we notice that the three elements of the Sylow 3-subgroup better be the identity, some element of $GL_2(\mathbb{Z}_3)$ and its inverse. That is, we need a group that is generated by a single element and is of order 3. We notice that we can get

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\}$$

as the first Sylow 3-subgroup. The others will just be conjugacy classes of this. In particular,

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\} \quad \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \right\} \quad \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \right\}$$

will be the other Sylow 3-subgroups. This is all there are, since anyother combination of entries will not be cyclic and of order 3.

Question 2

(a) To prove the correspondance theorem, we need to construct the appropriate subgroup structure. Suppose $\bar{H} \leq G/N$, and further suppose $a, b \in \bar{H}$. Then, since this is a coset subgroup, we know that $\exists g, h \in G$ such that $a = gN$ and $b = hN$. Since these representatives are in G , we can form a subset of G , call it H which contains all representatives of the cosets in \bar{H} . Now, clearly $H \subset G$, and we can see that if $g, h^{-1} \in H$, then

$$(gN)(h^{-1}N) = (gh^{-1})N \in \bar{H}$$

because \bar{H} is a subgroup. Then, by definition of H , $gh^{-1} \in H \forall g, h \in H$. Thus, we can conclude that $H \leq G$, $N \subset H$ and $\bar{H} = H/N$.

(b) Suppose that $\bar{H} \trianglelefteq G/N$. By the correspondance theorem, we know that $\exists H \leq G$ such that $\bar{H} = H/N$. To see that H is also normal in G , we use the normality of the quotient. That is, suppose $g \in G$ and $h \in H$, then

$$(gN)(hN)(g^{-1}N) = (gh^{-1}g)N \in \bar{H}$$

by normality of \bar{H} . So, this implies that $ghg^{-1} \in H$, and hence H is normal in G , with $N \subset H$.

(c) Since $p \mid |G|$, we can suppose $|G| = p^n m$ where $p \nmid m$. Then, we consider the three cases caused by Lagrange's Theorem, ignoring the trivial case of $|N| = 1$, since then we just get back G in the quotient and of course the number of Sylow p -subgroups will be equivalent. Instead:

Case 1: Suppose $|N| \mid p$. Well, then $|N| \nmid m$, and $|N| \leq p^n$. Thus, we get that $|N| = p^k$, for $k \leq n$. So, we have that $|G/N| = |G|/|N| = p^{n-k}$, and clearly p divides this, so we apply our Sylow theory to this new group. In particular, we notice by correspondance, that every p -subgroup of G/N will correspond with the quotient of a subgroup of size p^n in G , and hence a Sylow p -subgroup of G . Thus, if \bar{n}_p is the number of Sylow p -subgroups of G/N , we have that $\bar{n}_p \leq n_p$. When $n = k$, we have a quotient group of a size that is not divisible by p , and hence by Lagrange's Theorem can not have Sylow p -subgroups.

Case 2: Suppose $|N| \mid m$, then $|N| \nmid p$. Suppose $m/|N| = q < m$, then $|G/N| = |G|/|N| = p^n m/|N| = p^n q$. So, we can again apply our Sylow theory, and we see that

$$\bar{n}_p \mid q \quad n_p \mid m \quad \& \quad \bar{n}_p = n_p = 1 \pmod{p}.$$

But, obviously $q \mid m$, and $q < m$, so we must have that $\bar{n}_p < n_p$.

Case 3: Suppose $|N| \mid p^n m$, that is, $p^n m/|N| = p^k q$, for some $k \leq n$ and $q \leq m$, and $q \mid m$. The case when $|N| = |G|$ is ignored, since then we also get the trivial result of the quotient group being just the identity. Further, if $k = n$, we will get **Case 2**, and if $q = m$ we will get **Case 1**, so we can assume that $k < n$ and $q < m$. Then, we see that the quotient group is divisible by p and hence by Sylow theory, we know that there

are Sylow p -subgroups. Suppose there are \bar{n}_p of them, then

$$\bar{n}_p \mid q - n_p \mid m - 1 \quad \& \quad \bar{n}_p = n_p = 1 \pmod{p}.$$

Like **Case 2**, we must have that $\bar{n}_p < n_p$, as expected.

Question 3

(a) With $n = 2$, we see that $H_1 \cap H_2 = \{e\}$, but both subgroups are normal in G . Then, we know that the two commute with one another. To see this, consider $h_1 \in H_1$ and $h_2 \in H_2$, then it suffices to show that $h_1^{-1}h_2^{-1}h_1h_2 \in H_1 \cap H_2$, since $h_1^{-1}h_2^{-1}h_1h_2 = e \implies h_1h_2 = h_2h_1$. Notice

$$(h_1^{-1}h_2^{-1}h_1)h_2 \in H_2 \quad \& \quad h_1^{-1}(h_2^{-1}h_1h_2) \in H_1$$

by normality, and hence the commutivity follows. Now that we know this, the construction of the isomorphism becomes much easier. We use the natural homomorphism,

$$\varphi : H_1H_2 \rightarrow H_1 \times H_2 \quad \varphi(h_1h_2) \mapsto (h_1, h_2) \quad h_1 \in H_1, h_2 \in H_2.$$

To see this is a homomorphism, take $g_1 \in H_1$ and $g_2 \in H_2$ along with h_1 and h_2 to see

$$\varphi(h_1h_2g_1g_2) = \varphi(h_1g_1h_2g_2) = (h_1g_1, h_2g_2).$$

Next we need a bijection. Surjection follows trivially since if $(h_1, h_2) \in H_1 \times H_2$, we have $\varphi(h_1h_2) = (h_1, h_2)$ by construction. On the other hand, we have injection from definition as well,

$$\varphi(h_1h_2) = \varphi(g_1g_2) \iff (h_1, h_2) = (g_1, g_2) \iff h_1 = g_1, h_2 = g_2.$$

So, $H_1H_2 \cong H_1 \times H_2$.

(b) Suppose every Sylow subgroup of G is normal. Then, by Sylows Second theorem, we have that there is only one of each p dividing G . Further, this implies that each Sylow subgroup has trivial intersection with the other. Suppose $\{P_i\}_{i \in I}$, for I some indexing set, is the set of all Sylow subgroups of G , then we have just concluded that each is unique in its order from the others and $P_i \cap P_j = \{e\} \forall i, j \in I$ where $i \neq j$. Then, since we can apply the above lemma to get that

$$\prod_{i \in I} P_i \cong \times_{i \in I} P_i$$

we just need that the LHS is G . Notice that the order of the LHS will be the product of the subgroup sizes, but that is exactly $|G|$, so thus LHS is G .

Now, suppose that *not* every Sylow subgroup is normal. In particular, if $P_j \leq G$ is such a Sylow subgroup, then in the set of all Sylow subgroups of G , $\{P_i\}_{i \in I}$ for some $j \in I$. Then, since P_j is not normal, the subgroup is not unique as that Sylow subgroup, and will have non-trivial intersection with some other Sylow subgroup. Thus, the product of the subgroups will have an order different from that of $|G|$, and hence can not be isomorphic to G . Thus, by contrapositive, the claim follows.

Question 4

Notice that $175 = 5^2 \cdot 7$. We clearly need to apply Sylow theory, so we use the third theorem to get

$$n_7 = 1 \pmod{7} \quad n_7 \mid 25 \quad \& \quad n_5 = 1 \pmod{5} \quad n_5 \mid 7.$$

We see that we only actually have one option for each, that is $n_7 = n_5 = 1$. So, we have that each subgroup is normal, and since they are normal and will intersect trivially, we have from the previous lemma

$$G = H_5 H_7 \cong H_5 \times H_7.$$

We know that $|H_5| = 25$ and $|H_7| = 7$, so we see that since 7 is prime, by Lagrange's theorem $H_7 \cong \mathbb{Z}_7$, and thus we have

$$G \cong H_5 \times \mathbb{Z}_7.$$

Further, we recall that groups of order p^2 , for p prime are just $\mathbb{Z}_p \times \mathbb{Z}_p$, so

$$G \cong \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7.$$

As required.