1. (DF4.5.40) Prove that the number of Sylow p-subgroups of $GL_2(\mathbb{F}_p)$ is $p+1$. [Exhibit two distinct Sylow p-subgroups.]

Proof. Let P be any Sylow p-subgroup of $GL_2(\mathbb{F}_p)$ where p is prime.

The number of Sylow p-subgroups of $GL_2(\mathbb{F}_p)$ is the index in G of the normalizer $N_{GL_2(\mathbb{F}_p)}(P)$. The order of $GL_2(\mathbb{F}_p)$ is (by an earlier result) $(p^2-1)(p^2-p) = (p+1)(p-1)^2p$, so the order of P must be p. Hence P is cyclic.

Consider the Sylow p-subgroup

$$Q = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & p-1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

of $GL_2(\mathbb{F}_p)$. Consider conjugating the given generator of Q by an arbitary matrix

$$S = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

and identify the form of a matrix belonging to the normalizer $N_{GL_2(\mathbb{F}_p)}(Q)$. We have

$$\begin{aligned} S \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} S^{-1} &= (ad-bc)^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ &= (ad-bc)^{-1} \begin{pmatrix} ad-ca-cb & a^2 \\ -c^2 & -bc+ac+ad \end{pmatrix}; \end{aligned}$$

and if we demand that $S \in N_{GL_2(\mathbb{F}_p)}(Q)$, we have that

$$(ad-bc)^{-1} \begin{pmatrix} ad-ca-cb & a^2 \\ -c^2 & -bc+ac+ad \end{pmatrix} = \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}$$

for $1 \leq q \leq p-1$, as conjugation must send a generator of Q to another generator of Q. This occurs if and only if $c = 0$ and $a, d \neq 0$, in which case we find that

$$\begin{pmatrix} 1 & ad^{-1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}.$$

Hence

$$N_{GL_2(\mathbb{F}_p)}(Q) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : b \in \mathbb{F}_p,\ a, d \in \mathbb{F}_p^\times \right\}.$$

Since $|\mathbb{F}_p| = p$ and $\left|\mathbb{F}_p^\times\right| = p-1$, there are p options for b and $p-1$ options each for a and d so that $\left|N_{GL_2(\mathbb{F}_p)}(Q)\right| = (p-1)^2p$. Hence the number of Sylow p-subgroups of $GL_2(\mathbb{F}_p)$ is

$$\left|GL_2(\mathbb{F}_p) \colon N_{GL_2(\mathbb{F}_p)}(Q)\right| = \frac{(p+1)(p-1)^2p}{(p-1)^2p} = p+1.$$

□

To exhibit two distinct Sylow p-subgroups, conjugate one subgroup by a matrix which does not normalize that group. For instance, using the same subgroup

$$Q = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle,$$

we conjugate its generator by the matrix

$$T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

so that

$$\begin{aligned} T \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} T^{-1} &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}. \end{aligned}$$

Then

$$Q = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & p-1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

and

$$TQT^{-1} = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}, \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix}, \ldots, \begin{pmatrix} -(p-2) & p-1 \\ -(p-1) & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

are distinct Sylow p-subgroups of $GL_2(\mathbb{F}_p)$.

2. (Auxiliary result for DF4.5.50) Let H be a subset of G and let $a \in G$. Then $N_G(aHa^{-1}) = aN_G(H)a^{-1}$.

Proof. Let H, G, and $a \in G$ be as given. We have that $aN_G(H)a^{-1} = \{axa^{-1} : x \in N_G(H)\}$, and we check that any element axa^{-1} with $x \in N_G(H)$ sends aHa^{-1} to itself by conjugation. Indeed,

$$axa^{-1}aHa^{-1}(axa^{-1})^{-1} = axa^{-1}aHa^{-1}ax^{-1}a^{-1} = axHx^{-1}a^{-1} = aHa^{-1},$$

so that $aN_G(H)a^{-1} \subseteq N_G(aHa^{-1})$

Similarly, $N_G(aHa^{-1}) = \{x \in G : xaHa^{-1}x^{-1} = H\}$. With $x \in N_G(aHa^{-1})$, if $a^{-1}xa \in N_G(H)$, then $N_G(aHa^{-1}) \subseteq aN_G(H)a^{-1}$, which follows since

$$a^{-1}xaH(a^{-1}xa)^{-1} = a^{-1}xaHa^{-1}x^{-1}a = a^{-1}aHa^{-1}a = H.$$

Hence $N_G(aHa^{-1}) = aN_G(H)a^{-1}$. □

3. (DF4.5.50) Prove that if U and W are normal subsets of a Sylow p-subgroup P of G then U is conjugate to W in G if and only if U is conjugate to W in $N_G(P)$. Deduce that two elements in the center of P are conjugate in G if and only if they are conjugate in $N_G(P)$. (A subset U of P is normal in P if $N_P(U) = P$.)

Proof. Let U and W be normal subsets of a Sylow p-subgroup P of G as given.

Suppose that U is conjugate to W in $N_G(P)$, so that there exists $n \in N_G(P)$ such that $nUn^{-1} = W$. Clearly $n \in G$, so U is conjugate to W in G.

Conversely, suppose that U is conjugate to W in G, so that there exists $g \in G$ such that $gUg^{-1} = W$. Then by using the auxiliary result, we have that

$$gPg^{-1} = gN_P(U)g^{-1} \leq gN_G(U)g^{-1} = N_G(gUg^{-1}) = N_G(W).$$

Because $gPg^{-1} \leq N_G(W) \leq G$ and both P, gPg^{-1} are Sylow p-subgroups of G, it follows that P, gPg^{-1} are Sylow p-subgroups of $N_G(W)$ and so are conjugate to each other in $N_G(W)$. There exists $n \in N_G(W)$ such that $P = ngPg^{-1}n^{-1} = ngP(ng)^{-1}$, and so $ng \in N_G(P)$.

Since $gUg^{-1} = W$ and $n \in N_G(W)$, we have

$$ngU(ng)^{-1} = ngUg^{-1}n^{-1} = nWn^{-1} = W,$$

so that ng sends U to W by conjugation. Since $ng \in N_G(P)$, we have that U is conjugate to W in $N_G(P)$.

The center $Z(P)$ is normal in P, so that the singleton subsets $U = \{u\}$ and $W = \{w\}$ of $Z(P)$ are normal subsets of P. It follows by the above result that the two elements $u, w \in Z(P)$ are conjugate (since the singleton sets U and W are conjugate) in G if and only if they are conjugate in $N_G(P)$. □

4. (DF5.4.7) Prove that if p is a prime and P is a non-abelian group of order p^3 then $P' = Z(P)$.

Proof. Let P be a non-abelian group of order p^3 with p prime as given. Observe that P is a p-group so it has a nontrivial center $Z(P)$; furthermore P is non-abelian so $Z(P) \neq P$. This means that $|Z(P)|$ is either of order p or p^2. But if $|Z(P)| = p^2$, then $|P/Z(P)| = p$, which means $P/Z(P)$ is cyclic. By a previous result we know this would imply that P is abelian, a contradiction. Hence $Z(P)$ is of order p.

The quotient $P/Z(P)$ has order p^2, which by a previous result, we have that $P/Z(P)$ is abelian. Therefore, $P' \leq Z(P)$ (by Proposition 7). Since P is non-abelian, we have that P' is nontrivial and so we must have that $|P'| \geq p$, so that $P' = Z(P)$ as desired. □

5. (DF5.5.8) Construct a non-abelian group of order 75. Classify all groups of order 75 (there are three of them).

Given Z_3 which has order 3 and $Z_5 \times Z_5$ which has order 25, we wish to take the semidirect product $(Z_5 \times Z_5) \rtimes Z_3$ with respect to the (nontrivial) homomorphism $\varphi\colon Z_3 \to \mathrm{Aut}(Z_5 \times Z_5)$ which sends the nontrivial elements of Z_3 (which have order 3) to automorphisms of $Z_5 \times Z_5$ of order 3. The choice of taking the product is motivated by the fact that in a group of order 75, the number of Sylow 5-subgroups must be 1 (since this number must divide 3), and hence the group of order 25 must be normal in the group of order 75. Furthermore, the group of order 25 and the group of order 3 intersect trivially since their orders are coprime.

Note that the order of $\mathrm{Aut}(Z_5 \times Z_5)$ is the order of $GL_2(\mathbb{F}_5) = (5^2-1)(5^2-5) = 24 \cdot 20 = 480$, which is divisible by 3. By Cayley's theorem, $\mathrm{Aut}(Z_5 \times Z_5)$ has a subgroup of order 3, so there exist automorphisms of order 3 in $\mathrm{Aut}(Z_5 \times Z_5)$.

What remains is to exhibit an automorphism of $Z_5 \times Z_5$ of order 3, and send a nontrivial element of Z_3 to this automorphism via φ. Because $\mathrm{Aut}(Z_5 \times Z_5) \cong GL_2(\mathbb{F}_5)$, it suffices to find a non-identity matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

where $a, b, c, d \in \mathbb{F}_5$ and $ad - bc \neq 0$, such that $A^3 = I$. By expanding out A^3 and setting it equal to I, we have

$$\begin{pmatrix} a^3 + 2abc + bcd & b(a^2 + ad + bc + d^2) \\ c(a^2 + ad + bc + d^2) & abc + 2bcd + d^3 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 5.$$

We cannot have that $b \equiv c \equiv 0$, since it forces $a \equiv d \equiv 1$ (there are no elements of order 3 in $Z_5^\times$), which forms the identity matrix. So $b \not\equiv 0$ and $c \not\equiv 0$. Then simplify the problem by taking $d \equiv 0$; this is a guess/ansatz made in order to simplify the algebra. With these choices, the following system of congruences is formed:

$$\begin{aligned} a^3 + 2abc + bcd &\equiv \boxed{a^3 + 2abc \equiv 1} \\ a^2 + ad + bc + d^2 &\equiv \boxed{a^2 + bc \equiv 0} \\ abc + 2bcd + d^3 &\equiv \boxed{abc \equiv 1} \end{aligned}$$

Substituting the third congruence into the first congruence and simplifying yields $a^3 \equiv 4$, and by inspecting the values z^3 for $z \in \mathbb{F}_5$, we find that only $a \equiv 4$ will satisfy the congruence. Then the second congruence with $a \equiv 4$ yields $bc \equiv 4$, and there are many choices of b and c which satisfy this congruence. We take $b \equiv 2$ and $c \equiv 2$ for sake of example. Thus an automorphism of $\mathrm{Aut}(Z_5 \times Z_5)$ of order 3 may be expressed in matrix form as

$$A = \begin{pmatrix} 4 & 2 \\ 2 & 0 \end{pmatrix},$$

and by sending one of the nontrivial elements of Z_3 to the preimage of A (under some isomorphism from $\mathrm{Aut}(Z_5 \times Z_5)$ to $GL_2(\mathbb{F}_5)$) via φ, the semidirect product $(Z_5 \times Z_5) \rtimes_\varphi Z_3$ is a group of order 75 which is not abelian because φ is not a trivial homomorphism.

The three groups of order 75 up to isomorphism are:

$$\begin{aligned} & Z_3 \times Z_{25} && \text{(abelian)} \\ & Z_3 \times Z_5 \times Z_5 && \text{(abelian)} \\ \text{with } \varphi \text{ not trivial} \quad & (Z_5 \times Z_5) \rtimes_\varphi Z_3 && \text{(non-abelian)} \end{aligned}$$

Proof. Let G be a group of order $75 = 3 \cdot 5^2$. Then the number of Sylow 5-subgroups is 1 because $1 + 5 = 6$ does not divide 3. Hence there is a normal Sylow 5-subgroup of order 25 in G.

The number of Sylow 3-subgroups is either 1 or 25. Suppose there is only one Sylow 3-subgroup. The Sylow 5-subgroup P_5 must intersect trivially with the Sylow 3-subgroup P_3 (as 3 and 25 are coprime, there could not be any elements in common). Furthermore, because both subgroups are normal then the elements of the Sylow 3-subgroup commute with the elements of the Sylow 5-subgroup (by a result proven on our midterm).

Hence G is isomorphic to the direct product of these two groups, since the map from $P_3 \times P_5$ to G sending $(x_1, x_2) \mapsto x_1 x_2$ is an injective homomorphism due to the fact that the order of an element of the form $x_1 x_2$ will be the product of the orders of x_1 and x_2 (these elements commute and their orders will be relatively prime). Thus the kernel of the homomorphism must be trivial, so the homomorphism is indeed injective. The order of $P_3 \times P_5$ is 75, the same size as G, so the homomorphism is also bijective as a result and so is an isomorphism.

There is only one group (cyclic) of order 3 up to isomorphism, Z_3, and there are two groups (both abelian) of order 25 up to isomorphism, so the only options for $P_3 \times P_5$ are $Z_3 \times Z_{25}$ and $Z_3 \times (Z_5 \times Z_5) \cong Z_3 \times Z_5 \times Z_5$. Both of these groups are abelian. By the Fundamental Theorem of Finitely Generated Abelian Groups, we also know that these are the only abelian groups of order 75.

Suppose there are 25 Sylow 3-subgroups. We cannot say in this case that a given Sylow 3-subgroup is normal in G. But because the Sylow 5-subgroup P_5 is normal in G and for the same reason as above that P_5 intersects trivially with any Sylow 3-subgroup $P_3 \cong Z_3$, we have that

$$P_5 \rtimes P_3 \cong G.$$

Suppose that P_5 is isomorphic to Z_{25}. Then the order of $\mathrm{Aut}(Z_{25})$ is $\phi(25) = 20$ (ϕ is the Euler totient function), and so there are no automorphisms of order 3 of Z_{25}. This means any semidirect product of $Z_{25} \rtimes_\varphi P_3 \cong Z_{25} \rtimes_\varphi Z_3$ will be an abelian group of order 75 as the homomorphism φ must be trivial.

Thus for a non-abelian semidirect product we ought to take $P_5 \cong Z_5 \times Z_5$; and observe that we have already constructed above a non-abelian group of order 75 via a semidirect product $(Z_5 \times Z_5) \rtimes Z_3$. It remains to show that this is the only non-abelian group of order 75. Observe that for any nontrivial homomorphisms φ and ϕ from $Z_3 \to \mathrm{Aut}(Z_5 \times Z_5)$, $\varphi(Z_3)$ is conjugate to $\phi(Z_3)$. We can see this as the corresponding isomorphic subgroups in $GL_2(\mathbb{F}_5)$ of $\varphi(Z_3)$ and $\phi(Z_3)$ contain only the identity, a matrix, and its inverse, and so we may find a suitable change of basis matrix to conjugate one subgroup into the other.

Thus, by a proposition proved in class, it did not matter which nontrivial homomorphism φ from $Z_3 \to \mathrm{Aut}(Z_5 \times Z_5)$ we used in the semidirect product, and so the non-abelian group constructed earlier is the only one up to isomorphism.

Thus there are only three groups of order 75 as outlined above. □