411 Individual HW9

Jack Madden

December 2023

Problem 1

a) First, it is clear that the identity e is in $N_G(H)$, as $eHe = H$. Also, if $g \in N_G(H)$, we have that $gHg^{-1} = H$, and then after algebraic manipulation, we get $H = g^{-1}Hg$, which implies that $g^{-1} \in N_G(H)$. Finally, if $g, k \in N_G(H)$, we have that $gHg^{-1} = H$, $kHk^{-1} = K$. We then have $gkHk^{-1}g^{-1} = gHg^{-1} = H$, which implies that $gk \in N_G(H)$, which shows that the subgroup is closed.

b) Let X be the set of $p-$subgroups in G, under the action of conjugation. We know the action is well defined because, conjugating a subgroup by the identity gives that subgroup back and the associativity comes from the fact that the multiplication of group elements is associative. We have that $H \in X$. By the second Sylow Theorem, we know that $Orb(H) = X$. We also have that $Stab(H) = N_G(H)$. From this, we have that

$$|X| = |Orb(H)| = \frac{|G|}{|N_G(H)|} = [G : N_G(H)]$$

This tells us that $[G : N_G(H)]$ is equal to $|X|$, meaning it is equal to the number of $p-$subgroups in G.

c) We know that $H \in N_G(H)$, because conjugation of a group by an element in the group is an automorphism. So H is a $p-$subgroup of $N_G(H)$. Suppose another $p-$subgroup $K \in N_G(H)$, $K \neq H$. Then $aHa^{-1} = K$ for some $a \in N_G(H)$, by the 3rd Sylow theorem. But $aHa^{-1} = H$. Contradiction. Thus H is unique.

Problem 2

a) The prime factorization of $\left|(\mathbb{Z}_{2023})^{2023}\right|$ is $\left(17^2 \cdot 7\right)^{2023}$. We know that sylow $p-$subgroups of orders 17^{4046} and 7^{2023} exist, and that they will all be conjugate to eachother. But since the group is Abelian, a $p-$subgroup can only conjugate to itself. Therefore, there will be only 2 p-subgroups.

b) We have that the prime factorization of $|S_4|$ is $3 \cdot 2^3$. So our p-subgroups have order 3 or 8. We first examine the p subgroup of order 3. We contend that there are 4 such subgroups, $\langle(1\ 2\ 3)\rangle, \langle(1\ 2\ 4)\rangle, \langle(1\ 3\ 4)\rangle, \langle(2\ 3\ 4)\rangle$. This makes sense as 1 is congruent to 4 mod 3, and because 4 divides 2^3. Since the p-subgroups constitute an orbit under the group action of conjugation of subgroups, and the order of orbit must divide the order of the group, we see that there cannot be 7, 10, 13, 16, 19, or 22 subgroups of order 3.

   Next, we move to the subgroups of order 2^3. We contend that 3 such subgroups exist. First, we know that there cannot exist only 1 such subgroup, as this would imply that the subgroup of order 8 is normal. This cannot be true, as a normal subgroup is a union of conjugacy classes, and the conjugacy classes of S_4 have orders 6, 8, 3, 6, and 1. There is no way to add these numbers while including the identity and reaching a set of order 8. Also, since the p-subgroups constitute an orbit under the group action of conjugation of subgroups, and the orbit must divide the order of the group, we observe that $5, 7, 9, \cdots 23$ do not divide 24, the order of the group. So 3 such subgroups exist.

c) We have that the prime factorization of $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$. We first find how many subgroups of order $2^2 = 4$ exist. We contend that there are 5 subgroups, and that these subgroups are isomorphic to the Klein-4 group, and that their normalizers are subgroups of A_5 isomorphic to A_4.

   We then turn to the subgroups of order 3. By Sylow-3 we know that be 1, 4, or 10 subgroups of order 3, as these are the numbers that are congruent to 1 mod 3, and also divide 20. We know that there cannot only be 1, as this would imply that there was a normal subgroup of order 3 in A_5, which cannot be the case, as A_5 is simple. We contend that there are therefore 10 such subgroups, which are generated by 3-cycles in A_5. We know that there are 20 3 cycles in A_5, by counting $\frac{5 \cdot 4 \cdot 3}{3}$, and they can be partitioned into pairs along with the identity such as $\{Id, (1\ 2\ 3), (1\ 3\ 2)\}, \{Id, (1\ 2\ 4), (1\ 4\ 2)\}$ and so on. Since there are at most 10 subgroups of this order, we know that we have found them all.

   We then turn to the subgroups of order 5. We know that the number n must be congruent to 1 mod 5 and also must divide 12. Thus, our only two options are 1 or 6. But if there was only 1, this would imply a subgroup that was only conjugate to itself by Sylow 2 and therefore normal. However this would be a non-trivial normal subgroup which we know does not exist as A_5 is simple. Thus, 6 such subgroups exist.

Problem 3

a) We know from Practice Midterm 2, Problem 5, that G is either abelian, or $G/Z(G)$ is not Abelian. Since $Z(G)$ is a subgroup of $|G|$, by Lagrange's theorem, it has order $1, p$, or p^2. If it has order p, then $G/Z(G)$ has order p^2/p, and is therefore cyclic, meaning that the group is Abelian, and therefore

$|Z(G)| = p^2 \neq p$. So this cannot be the case. If it has order 1, by the class equation we have that $|G| = 1 + p(k)$, for some $k \in \mathbb{Z}$, as was proven in problem 9 on the last homework. But then the order of G is congruent to 1 mod p, when in reality the order of G is divisible by p contradiction. So $|Z(G)| = p^2$ and therefore $|G|$ is Abelian. Since it is Abelian, and of order p^2, by the theorem of finitely generated Abelian groups we know that G is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

b) Take $p = 2$, then $p^3 = 8$. The group D_4 has order 8 and is non-abelian.

Problem 4

a) Call X the set of conjugate p-subgroups and let the elements of H act on them by conjugation. Suppose that for $H_1 = H, H_2, H_1 \neq H_2 \in X$ that $Stab(H_1) = Stab(H_2)$. This tells us that

$$hH_2h^{-1} = H_2$$

for any $h \in H$. This tells us that $H \leq N_G(H_2)$. We also have that H_2 is normal in $N_G(H_2)$ as it is contained in $N_G(H_2)$, and for any $h_n \in N_G(H_2)$, $h_nH_2h_n^{-1} = H_2$. But then H, H_2 are both $p-$subgroups in $N_G(H_2)$ and therefore must be conjugate. But since H_2 is normal in $N_G(H_2)$, this cannot be the case unless $H_1 = H = H_2$. From this, we have that the orbit of any element $H_i \neq H$ is

$$\frac{|H|}{|Stab(H_i)|}$$

But since $Stab(H_i) \neq H$, we have that it must be a subgroup of H and then can have order at most p^{k-1}, where $|H| = p^k$, by Lagrange's theorem. Thus, its orbit will be divisible by p.

b) We know that $|X|$ is equal to the sum of the sizes of its orbits. By the result obtained in (a), every orbit will be divisible by p, except for one orbit of order 1. Thus:

$$|X| = 1 + p(Orb(H_1)) + p(Orb(H_2)) + \cdots = 1 + p(k)$$

for some k and thus $|X|$ is congruent to 1 mod p.

Problem 5

a) By Cauchy's theorem, since 2 is a prime dividing the order of the group, $2p$, there exists an element b of order 2. Likewise, since p is a prime dividing the order of the group, there exists an element a of order p.

b) The index of $\langle a \rangle = 2p/p = 2$. This means there are 2 cosets in the quotient group and thus the multiplication of either coset by an element not in it will yield the other coset, whether the multiplication is on the left or the right. Thus, from this we know that $\langle a \rangle$ is normal.

c) Since $\langle a \rangle$ is normal in G, we know that

$$bab^{-1} = a^k$$

for some k. Also, $b^{-1} = b$ so

$$bab = a^k$$

Then:

$$a = ba^k b$$

as we showed on midterm 1, this is equal to

$$a = (bab)^k$$

but $bab = a^k$ so then

$$a = (a^k)^k$$

or

$$a = a^{k^2}$$

thus, we have that k^2 congruent to 1 mod p, which implies that k is congruent to 1 or -1 mod p, meaning bab^{-1} is either a or a^{-1}

d) When $bab = a$, we have $ba = ab$. Since $\langle a \langle$ is normal, we have that $G/\langle a \rangle = \{\langle a \rangle, b\langle a \rangle\}$. Thus, every element of G can either be written as a power of b and a power of a. We observe recursively that

$$ba^k = baa^{k-1} = aba^{k-1} = \cdots = a^k b$$

Thus, for any two elements $x = b^m a^n, y = b^\ell a^k$, $m, n, \ell, k \in \mathbb{Z}$, we have that

$$xy = b^m a^n b \ell a^k = b^m a^k b^\ell a^n = b^\ell a^k b^m a^n = yx$$

Thus, $bab = a$ implies that the group is abelian. From this, we know that by the classification theorem of finite abelian groups that G must be isomorphic to $\mathbb{Z}_{2p}$ or $\mathbb{Z}_2 \times \mathbb{Z}_p$.

Now the other case, $bab = a^{-1}$, we have

$$(bab) = a^{-1}$$

raise both sides to an arbitrary power k, giving

$$(bab)^k = (a^{-1})^k$$

$$ba^k b = (a^k)^{-1}$$

$$ba^k = (a^k)^{-1} b$$

which implies that

$$ba^k = (ba^k)^{-1}$$

Thus, we have that every element in the coset $b\langle a \rangle$ is its own inverse, i.e. has order 2. From here, we can construct an isomorphism to D_p, where the p rotations are the elements of $\langle a \rangle$, and the p reflections are the elements of $b\langle a \rangle$.

Problem 6

a) We know that this group action is valid, as the identity matrix takes every column vector to itself, and that the second axiom will also hold, as matrix multiplication is associative, which gives us that $(AB)x = A(Bx)$ where $A, B \in GL_n(\mathbb{F}_p), x \in (\mathbb{F}_p)^n$.

b) The two orbits are the zero vector, an orbit of all other vectors of size $p^n - 1$. We know that any non zero vector can be reached from any other non zero vector. This is because no non-zero vector is held constant by any matrix other than the identity. Thus, the stabilizer of any vector has order 1 and thus the orbit will be all the vectors.

c) We know that each element in $GL_n(\mathbb{F}_p)$ constitutes a bijection from the set of the non-zero column vectors to itself. This is because it is injective and surjective. Let x, y be in the set of column vectors, and let $M \in GL_n(\mathbb{F}_p)$. Then if $Mx = My$, we can multiply by M^{-1} on both sides which we know exists because $M \in GL_n(\mathbb{F}_p)$. Also, for any column vector y, we know that $M(M^{-1}y) = y$, so it is also surjective. Thus, since each element of $GL_n(\mathbb{F}_p)$ constitutes a bijection from a set of $p^n - 1$ elements to itself, there will be a homomorphism $\phi : GL_n(\mathbb{F}_p) \to S_{p^n-1}$. We know that the kernel of this homomorphism is just the identity matrix, which by the first isomorphism theorem tells us that G is isomorphic to $\phi(G)$. Since a homomorphism maps subgroups in one group to subgroups in another group, we know that $\phi(G)$ is a subgroup of S_{p^n-1}, and by the first isomorphism theorem G isomorphic to a subgroup in S_{p^n-1}.

d) See picture at https://imgur.com/a/eXbi0QV

Problem 7

a) see image at https://imgur.com/a/eXbi0QV

b) We see that each node in the graph has 3 edges emerging from it. We know that this is also the maximum number of lines it can participate in as once you linearly combine a vector with a second vector, the 3rd vector in the line is implicitly defined. Thus, one vector can only participate in 3 lines.

c) We know that there are 7 lines. We also know that the order of the group $GL_3(\mathbb{F}_2)$ is 168. From this, to show that the group action is transitive, we must show that the stabilizer of a line L, $Stab(L)$ has order 24, as $Stab(L) \cdot Orb(L) = |GL_3(\mathbb{F}_2)| = 168$. We choose the following line:

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \right\}$$

We construct a matrix that sends each element in L to itself. This was done by starting with every element in the matrix being free, and seeing that all elements other than g and h must have a fixed value to send each element in L to itself and also fulfill the . Thus, we observe that there are 4 matrices which send L to itself as g and h can each be chosen in 2 ways.

$$\begin{bmatrix} 1 & 0 & g \\ 0 & 1 & h \\ 0 & 0 & 1 \end{bmatrix}$$

The next observation we made was that the action of the stabilizer on L is essentially the permutations in S_3. We then map the result from problem $6d$ to get that:

$$\begin{bmatrix} 0 & 1 & g \\ 1 & 1 & h \\ 0 & 0 & 1 \end{bmatrix} \cong (L_1\ L_2\ L_3)$$

$$\begin{bmatrix} 1 & 1 & g \\ 1 & 0 & h \\ 0 & 0 & 1 \end{bmatrix} \cong (L_1\ L_3\ L_2)$$

$$\begin{bmatrix} 0 & 1 & g \\ 1 & 0 & h \\ 0 & 0 & 1 \end{bmatrix} \cong (L_1\ L_2)$$

$$\begin{bmatrix} 1 & 0 & g \\ 1 & 1 & h \\ 0 & 0 & 1 \end{bmatrix} \cong (L_1\ L_3)$$

$$\begin{bmatrix} 1 & 1 & g \\ 0 & 1 & h \\ 0 & 0 & 1 \end{bmatrix} \cong (L_2\ L_3)$$

Since g and h can be chosen 4 ways for each of the 6 matrices, this gives us a stabilizer that is 24 elements large. Thus,

$$7 = |Orb(L)| = \frac{168}{24} = \frac{|GL_3(\mathbb{F}_2)|}{|Stab(L)|}$$

. which implies that the group action is transitive.