MATH 411: INTRODUCTION TO ABSTRACT ALGEBRA
HOMEWORK #9

TRUNG DANG
33858723

Problem 1

Problem Statement: Let H be a subgroup of a group G. Define $N_G(H) = \{g \in G : gHg^{-1} = H\}$.

(1) Prove that $N_G(H)$ is a subgroup of G

(2) Suppose that H is a Sylow p-subgroup of G. Show that the number of Sylow p-subgroups of G is equal to $[G : N_G(H)]$

(3) Suppose that H is a Sylow p-subgroup of G. Prove that H is a unique Sylow p-subgroup of $N_G(H)$

Solution. (1) First, we observe that:

$$gHg^{-1} = H \Longleftrightarrow H = g^{-1}Hg$$

thus g^{-1} is also in $N_G(H)$.
Second, we observe that for $g_1, g_2 \in N_G(H)$, we have:

$$(g_2g_1)H(g_2g_1)^{-1} = g_2g_1Hg_1^{-1}g_2^{-1} = g_2Hg_2^{-1} = H$$

thus g_1g_2 is also in $N_G(H)$ Therefore, by the subgroup test we have $N_G(H)$ is a subgroup of G

(2) Let us define the action of conjugation from G on to the set S of all Sylow p-subgroups of G. Then observe that $N_G(H)$ is the stabilizer of the element H, and since for every $H_1, H_2 \in S, H_1$ is a conjugate of H_2, S is the orbit of the action. Therefore, by the orbit-stabilizer theorem, we have:

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

(3) Assume that there is another Sylow p-subgroup H' in $N_G(H)$. Then by the second Sylow theorem, we must have:

$$H' = gHg^{-1}, \text{ for some } g \text{ in } N_G(H)$$

But then by definition, for all $g \in N_G(H)$, $gHg^{-1} = H$, thus $H' = H$, a contradiction.
Hence, H is a unique Sylow p-subgroup of $N_G(H)$

■

Problem 2

Problem Statement: For every prime p, find the number of Sylow p-subgroups of:

(1) $(\mathbb{Z}_{2023})^{2023}$

(2) S_4

(3) A_5

Solution. (1) The order of $(\mathbb{Z}_{2023})^{2023}$ is $2023^{2023} = 7^{2023} \cdot 17^{4046}$. Notice that for every subgroup H of G, $N_G(H) = G$. Therefore, for $p = 7, 17$, the number of Sylow p-subgroup of $(\mathbb{Z}_{2023})^{2023}$ is both 1.

(2) The order of S_4 is $24 = 2^3 \times 3$.

- If p =2, then the Sylow 2-subgroup of S_4 has order 8. The number of Sylow 2-subgroup should also be divisible by 24 (as we have shown in class), and be an odd number (by the third Sylow theorem). Thus, there can only be either 1 or 3 Sylow 2-subgroups of S_4.
  But if there is only 1 Sylow 2-subgroups, then S_4 must have a normal subgroup (which it does not). Therefore, there must be 3 Sylow 2-subgroups
- If p =3, then the Sylow 3-subgroup of S_4 has order 3. By the same argument, we must have either 1 or 4 Sylow 2-subgroups. And we can prove that 4 subgroups are sufficient by listing them out: $\{Id, (123), (132)\}, \{Id, (134), (143)\}, \{Id, (124), (142)\}, \{Id, (234), (243)\}$.

(3) The order of A_5 is $60 = 2^2 \times 3 \times 5$.

- If p = 2 then the Sylow 2-subgroup of A_5 has order 4. One example of the Sylow 2-subgroup of A_5 is $\{Id, (12)(34), (14)(23), (13)(24)\}$. We can verify that $N_G(H) = 12$, and thus there are $[G : N_G(H)] = 5$ Sylow 2-subgroups of A_5.
- If p = 3 then the Sylow 3-subgroup of A_5 has order 3. Also the number of Sylow 3-subgroup of A_5 must divides 60 and is congruent to 1 mod 3. Thus, it can only be 1, 4, 10. And we can show that 10 is sufficient by listing all the subgroups of order 3 in A_5, namely $\{Id, (abc), (acb)\}$ for $1 \le a < b < c \le 5$
- If $p = 5$ then the Sylow 5-subgroup of A_5 has order 5. The number of Sylow 5-subgroup must also divides 60 and be congruent to 1 modulo 5. Therefore, it can only be 1, 6. We can prove that 6 is sufficient by listing all the 5-subgroups of A_5, namely the groups generated by 5-cycles.

$\blacksquare$

Problem 3

Problem Statement:

(1) Let G be a group of order p^2 where p is prime. Prove that G is an abelian group isomorphic to either $\mathbb{Z}_p \times \mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$

(2) Construct a non-abelian group of order p^3

Solution. (1) Let a be an arbitrary non-identity element of G. Then $ord(a)||G| = p^2$, thus, either $ord(a) = p$ or $ord(a) = p^2$.

- If there is an element a of order p^2, then $G =< a >\approxeq \mathbb{Z}_{p^2}$
- If there is no element a of order p^2, then for all $a \neq e \in G$, $ord(a) = p$, and $< a >\approxeq \mathbb{Z}_p$. Then consider the group $G/ < a >$ of order p. Then this group is also isomorphic to $\mathbb{Z}_p$. Thus, $G \approxeq< a > \times G/ < a >\approxeq \mathbb{Z}_p \times \mathbb{Z}_p$

(2) Consider the group D_4 of order $8 = 2^3$, which is non-Abelian and of order p^3 for $p = 2$

■

Problem 4

Problem Statement: Let G be a finite group and let H be its Sylow p-subgroup. Consider the conjugation action of H on the set of all Sylow p-subgroups $\{H_1, \cdots, H_n\}$

(1) Show that every orbit of this action has size divisible by p except for one orbit which has size 1

(2) Deduce from (a) that the number of Sylow p-subgroups is congruent to 1 modulo p

Solution. (1) First, observe that for all subgroups $H \in G$, we have $H \subseteq N_G(H)$. Now, let H be an arbitrary Sylow p-subgroup of G, wherein $|G| = p^k m$ and $|H| = p^k$. Let S be the set of all Sylow p-subgroups and let us define the action $H \curvearrowright S$ to be gS_1g^{-1} for $g \in H, S_i \in S$. Then, let T be the set of all fixed elements of this action, that is S_i such that $N_H(S_i) = H$. Let P be an element of T.
Then, we have:

- $H = N_H(S_i) \subseteq N_G(S_i)$
- $N_G(S_i)$ is a subgroup of G (by problem 1)
- $S_i \subseteq N_G(S_i)$, so H and S_i are conjugates in $N_G(S_i)$
- But S_i is also normal in $N_G(S_i)$

Therefore $H = S_i$, or $T = \{H\}$. Using the Orbit-Stabilizer theorem, we can therefore conclude that this action has every orbit of size divisible by p except for one orbit of size 1.

(2) And since the orbits are either equal or disjoint, the number of Sylow p-subgroups is congruent to 1 modulo p.

$\blacksquare$

Problem 5

Problem Statement: Let p be an odd prime and let G be a group of order $2p$.

(1) Prove G contains an element a of order p and an element b of order 2

(2) Prove: $< a >$ is normal in G

(3) Prove bab^{-1} is either equal to a or equal to a^{-1}

(4) Prove: In the first case of (3), $G \approxeq \mathbb{Z}_2 \times \mathbb{Z}_p \approxeq \mathbb{Z}_{2p}$. In the second case of (3), $G \approxeq D_p$

Solution. (1) By the first Sylow Theorem, there exists a Sylow p-subgroup A of order p and a Sylow p-subgroup B of order 2. And since they are subgroup of a prime order, then they must be isomorphic to the cyclic groups $\mathbb{Z}_p$ and $\mathbb{Z}_2$ respectively. Therefore, there is an element a of order p and an element b of order 2.

(2) let $< a >= A$. Then consider all Sylow p-subgroups $A_1, A_2, \cdots A_N$ in G. Then by the second Sylow theorem, we have $A_i = gA_jg^{-1}$ for all $i, j \in \{1, 2, 3, \cdots, N\}$ and for some $g \in G$. Thus, the Syllow p-subgroups form a single orbit of the conjugate action of G on the set of Syllow p-subgroups.
By the orbit stabilizer theorem, we have:

$$N | 2p$$

But by the third Sylow theorem, we have $N \equiv 1 \mod p$.
Thus, we can deduce that $N = 1$, or there is only one Sylow p-subgroup in G, namely A. Thus, for all $g \in G, gAg^{-1} = A$, hence $< a > \lhd G$

(3) Let $bab^{-1} = a^i$ for some $i = 0, 1, \cdots, p-1$. Then we have:

$$\begin{aligned} a = b^2ab^{-2} &= b(bab^{-1})b^{-1} = ba^ib^{-1} \\ &= ba(b^{-1}b)a(b^{-1}b)\cdots(b^{-1}b)ab^{-1} \\ &= (bab^{-1})(bab^{-1})\cdots(bab^{-1}) \\ &= (a^i)^i = a^{i^2} \end{aligned}$$

Thus, $i^2 \equiv 1 \mod p$, so either $i = 1$ or $i = -1$

(4) If $bab^{-1} = a$, then right multiplying both sides with b we have $ba = ab$, so a,b commutes. But then as we have shown in class, all the elements of G can be written as b^ia^j, where $i = 0, 1$ and $j = 0, 1 \cdots, p-1$. Therefore, G is Abelian, and is isomorphic to $\mathbb{Z}_{2p} \approxeq \mathbb{Z}_p \times \mathbb{Z}_2$

Else if $bab^{-1} = a^{-1}$, then we construct a bijection from $G \to D_p$ as follows:

- $a \to R =$ rotation by $\frac{2\pi}{p}$ degrees
- $a^i \to R_i = R^i$
- $b \to S =$ reflection by an axis

Then for $a^i b^j, a^k b^l \in G$, from part (c), we can verify that $a^i b^j a^k b^l = R^i S^j R^k S^l$
Therefore, $G \approxeq D_p$

■

Problem 6

Problem Statement:

(1) Check action axioms to prove that $GL_n(\mathbb{F}_p)$ acts on the set $(\mathbb{F}_p)^n$ of column-vectors

(2) Prove that the action in (a) has 2 orbits. How many elements are in each orbit?

(3) Use part (b) to show that $GL_n(\mathbb{F}_p)$ is isomorphic to a subgroup of S_{p^n-1}

(4) Prove $GL_2(\mathbb{F}_2) \approxeq S_3$

Solution. (1) We have:

- The identity of $GL_n(\mathbb{F}_p)$ is $e = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}$, or the $n \times n$ identity matrix, and so $\forall v \in (\mathbb{F}_p)^n, ev = v$
- for all $n \times n$ matrices A, B, we have:

$$\begin{aligned} AB \star v &= AB \cdot v(\mod p) \\ &= A \cdot (B \cdot v \mod p) \mod p \\ &= A \star (B \star v) \text{ (by normal matrix multiplication and modular arithmetic)} \end{aligned}$$

Therefore, the action satisfies the action axioms, thus $GL_n(\mathbb{F}_p)$ acts on the set $(\mathbb{F}_p)^n$ of column vectors

(2) The action has 2 orbits, namely $\{0\}$ and $(\mathbb{F}_p)^n\{0\}$. The former is obviously an orbit, as for all $A \in GL_n(\mathbb{F}_p)$, we must have $A \cdot \vec{0} = \vec{0}$. For the latter, take any 2 different vectors $\vec{v}, \vec{u}$. Because there are n variables and n equations, there exists a matrix A which is the solution of the system of equations:

$$\begin{cases} a_{11}u_1 + a_{12}u_2 + \cdots + a_{1n}u_n = v_1 \\ \cdots \\ a_{n1}u_1 + a_{n2}u_2 + \cdots + a_{nn}u_n = v_n \end{cases}$$

Therefore, all vectors except the zero vector form the second orbit, and it has size $p^n - 1$

(3) Let us define X to be the set of all column vectors in $(\mathbb{F}_p)^n$ except the zero vector. Then define the function $f : GL_n(\mathbb{F}_p) \to S_X$ to take $f(A) \to \{Av_1, Av_2, \cdots, Av_N\}$ where v_i are vectors in X. Then we will prove that all the possible permutations from f forms a subgroup Y of $S_X \approxeq S_{p^n-1}$. Indeed, we have: $f(A)f(B) = f(A)(\{Bv_1, Bv_2, \cdots, Bv_N\}) = \{ABv_1, ABv_2, \cdots, ABv_N\} \in Y$. Notice how this also provides us with a homomorphism. And since $A \in GL_n(\mathbb{F}_p)$, A is invertible, thus $A^{-1} \in GL_n(\mathbb{F}_p)$, so $f(A^{-1})$ is also in Y.
Thus Y is a subgroup of S_X.
It is apparent by normal matrix multiplication that $f(A) \neq f(B) \forall A \neq B \in X$, and by definition of Y that f is surjective. Thus f is bijective.
And since we have shown above that f is a homomorphism, it is also an isomorphism.

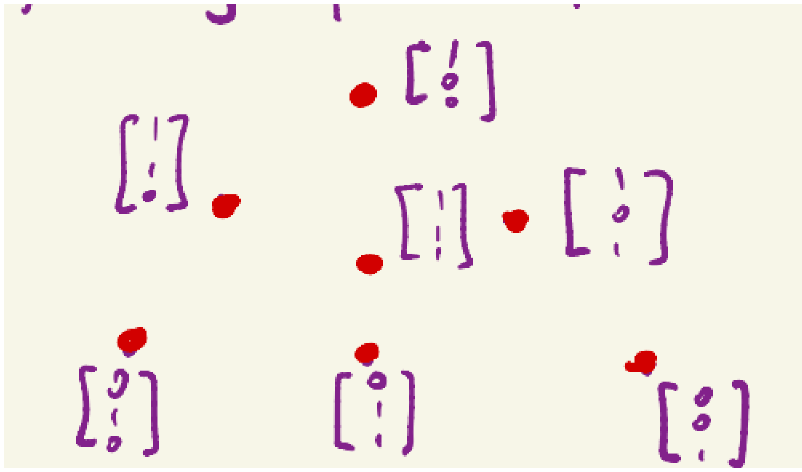
(4) From part (3) we have $GL_2(\mathbb{F}_2)$ is isomorphic to a subgroup of $S_{2^2-1} = S_3$. But then since the order of $GL_2(\mathbb{F}_2)$ is $(2^2-1)(2^2-2) = 6$, the subgroup it is isomorphic to must also have order 6. Thus this subgroup equals S_3.

$\blacksquare$

Problem 7

Problem Statement: A triple of non-zero vectors in $(\mathbb{F}_2)^3$ is called a line if they are linearly dependent.

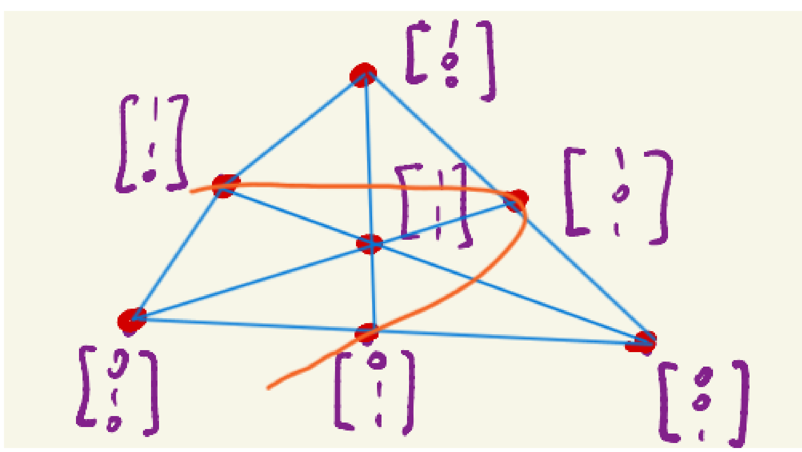
(1) Draw all lines using the following picture of non-zero vectors:



(2) Show that every non-zero vector is contained in exactly 3 lines

(3) Prove that the action of $GL_3(\mathbb{Z}_2)$ from problem 6(a) induces a transitive action of $GL_3(\mathbb{F}_2)$ on the set of lines

Solution. (1) There are 7 lines in the picture, as shown by 6 blue lines and 1 orange line in the annotated figure below:



(2) For a value in the vector to be 1, then the corresponding values in the other 2 vectors in the line must be 0 and 1, and for a value to be 0, then the corresponding value in the other 2 vectors must be either both 1 or both 0. In other words, once we have a vector, and we choose another vector, there is only one definite way to choose the third vector in line. Therefore, for each vector, we can only divide the other 6 vectors into 3 pairs, corresponding to 3 lines.

(3) By the orbit stabilizer Theorem, we have the number of elements in an orbit is

$$|Orb(x)| = \frac{|G|}{|G_X|} = \frac{7 \cdot 6 \cdot 4}{|G_X|}$$

Notice that:

- For a transformation matrix A and a line of 3 vectors a, b, c, we have $Aa + Ab = A(a+b) = Ac$, so the action maps a line to a line
- A matrix stabilizes a line if it maps the three vectors to a permutation of itself.

Using these 2 observations, we can verify on the line $\{[1,0,0],[1,1,0],[0,1,0]\}$, that there are 24 stabilizers, thus the orbit size of this action is 7, which is equal to the number of all lines.

Thus, the action is transitive.

$\blacksquare$