ALGEBRA: HOMEWORK 3

Problem 1. Determine all groups of order 18.

Proof. Assume G is a group of order 18. By Sylow's theorem G has a unique subgroup N_9 of order 9, and it is normal. We claim that

$$N_9 = C_9 \quad \text{or} \quad N_9 = C_3 \times C_3.$$

Proof of claim: In class we have proved such a result: if $|G| = p^k$, then $p \mid |Z(G)|$. So $|Z(N_9)| = 3$ or 9. If N_9 has an element of order 9, then $N_9 \cong C_9$. If not, then every nonunit element has order 3. Pick a nonunit element $g \in Z(N_9) \subset N_9$, and an $h \in N_9 \setminus < g >$. It is easy to prove $\{g^i h^j\}$ with $0 \le i \le 2, 0 \le j \le 2$ are mutually distinct and thus exhaust elements in N_9. Since $g \in Z(N_9)$, the group multiplication with elements in $\{g^i h^j\}$ is commutative. So N_9 is abelian isomorphic to $< g > \times < h > \cong C_3 \times C_3$. $\square$

Now we consider cases:

(1) $N_9 =< g > \cong C_9$, by Sylow's theorem, there exists an element h of order 2. Assume $hgh^{-1} = hgh = g^k$ with $1 \le k \le 8$. Then $g^{k^2} = (g^k)^k = (hgh)^k = hg^k h = g$, and then $g^{(k-1)(k+1)} = e$, and then $k = 1$ or $k = 8$. If $k = 1$, $gh = hg$, and $G =< g > \times < h >$ and is abelian. If $k = 8$, $hgh = g^{-1}$, and G is isomorphic to the dihedral group D_{18}.

(2) $N_9 =< g > \times < h > \cong C_3 \times C_3$. By Sylow's theorem, assume $x \in G$ is of order 2. Assume $xgx = g^a h^b$ and $xhx = g^c h^d$. Then by

$$\begin{aligned} g =& x(xgx)x = x(g^a h^b)x = g^{a^2+bc} h^{(a+d)b} \\ h =& x(xhx)x = x(g^c h^d)x = g^{d^2+bc} h^{(a+d)c}, \end{aligned}$$

we have in modulo 3, $a^2 + bc = 1$, $(a+d)b = 0$, $d^2 + bc = 1$, $(a+d)c = 0$.

(i) If $a + d \ne 0$, then $b = c = 0$, $a = d \ne 0$. If $a = d = 1$, G is abelian and $G =< g > \times < h > \times < x > \cong C_3 \times C_3 \times C_2$. If $a = d = 2$, we have relations

$$g^3 = h^3 = e, xgx = g^2, xhx = h^2,$$

and can prove $G = \{g, h, x | g^3 = h^3 = x^2 = e, xgx = g^2, xhx = h^2\} =: E_{18}$, and an element in E_{18} has order 1 or 2 or 3.

(ii) $a + d = 0$, $a = d = 0$, then $b = c = 1$ or $b = c = 2$, and then

$x(gh)x = gh, x(gh^{-1})x = gh^{-1}$ or $x(gh)x = (gh)^2, x(gh^{-1})x = (gh^{-1})^2$.

Change variables as $\tilde{g} = gh, \tilde{h} = gh^{-1}$, and we have

$$x\tilde{g}x = \tilde{g}, x\tilde{h}x = \tilde{h}^2 \text{ or } x\tilde{g}x = \tilde{g}^2, x\tilde{h}x = \tilde{h}.$$

and $< g > \times < h > = < \tilde{g} > \times < \tilde{h} >$. W.L.O.G we may assume $x\tilde{g}x = \tilde{g}, x\tilde{h}x = \tilde{h}^2$. It is not hard to prove that $(\tilde{h}, x)$ generate a subgroup G_6 of order 6 and isomorphic to $D_6 \cong \mathcal{S}_3$. Since $\tilde{g}$ is commutable with $\tilde{h}$ and x, we have $G = < \tilde{g} > \times G_6 = C_3 \times \mathcal{S}_3$.

(iii) $a = 1, d = 2$ or $a = 2, d = 1$. W.L.O.G, we may assume $a = 1, d = 2$, then $b = 0$ or $c = 0$. There are 5 cases:
(1) $b = c = 0$, $G = C_3 \times \mathcal{S}_3$ by result in (ii).
(2) $b = 0, c = 1$, let $\tilde{h} = gh$ and consider $< g > \times < \tilde{h} >$ we will find $G = C_3 \times \mathcal{S}_3$.
(3) $b = 0, c = 2$, let $\tilde{h} = g^2h$ and consider $< g > \times < \tilde{h} >$ we will find $G = C_3 \times \mathcal{S}_3$.
(4) $b = 1, c = 0$, let $\tilde{g} = gh^2$ and consider $< \tilde{g} > \times < h >$ we will find $G = C_3 \times \mathcal{S}_3$.
(5) $b = 2, c = 0$, let $\tilde{g} = gh$ and consider $< \tilde{g} > \times < h >$ we will find $G = C_3 \times \mathcal{S}_3$.

In summary, G can be $C_{18}, D_{18}, C_3 \times C_3 \times C_2, \mathcal{S}_3 \times C_3$, or

$$E_{18} = \{g, h, x | g^3 = h^3 = x^2 = e, xgx = g^2, xhx = h^2\}.$$

□

Problem 2. Let p be a prime number. What is the order of $SL_2(\mathbb{Z}/p\mathbb{Z})$?

Proof. It is equivalent to ask how many solutions to $ad - bc = 1 \bmod(p)$. Just discuss in cases (i) $ad = 0$, (ii) $bc = 0$, (iii) $ad \neq 0, bc \neq 0$. The answer is $p^3 - p$. □

Problem 3. What is the index $(SL_2(\mathbb{Z}/p\mathbb{Z}) : \Gamma_0(p))$?

Proof. Just need to compute $|\Gamma_0(p)|$. This is equivalent to ask how many triples (a, b, d) satisfying $ad = 1 \bmod(p)$. The answer is $p(p-1)$, and $(SL_2(\mathbb{Z}/p\mathbb{Z}) : \Gamma_0(p)) = p + 1$. □

Remark 1.

$$\Gamma_0(p) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{Z}/p\mathbb{Z}, ad = 1 \right\} \subset SL_2(\mathbb{Z}/p\mathbb{Z}).$$

Problem 4. Realize $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ as subgroups of $GL_2(\mathbb{Z})$.

Proof. (1) $\mathbb{Z}/3\mathbb{Z}$:

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

(2) $\mathbb{Z}/4\mathbb{Z}$:

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

(3) $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$:

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

□

Problem 5. Find all subgroups of the symmetric group $\mathcal{S}_4$ of order 8.

Proof. $|\mathcal{S}_4| = 24$ and by Sylow's theorem there exist at most 3 subgroups of order 8. We can take $1, 2, 3, 4$ as 4 vertices on a square counterclockwise, then the induced dihedral group, which is isomorphic to D_8, can be viewed as a subgroup of $\mathcal{S}_4$. The elements are

$$\{Id, (1234), (4321), (13)(24), (12)(34), (23)(14), (13), (24)\}.$$

We can change the order of index of the square to (1243) and (1324), and obtain the other 2 subgroups of order 8. □

Problem 6. Assume that G is generated by two elements and that $\exp(G) = 3$, i.e., for every $g \in G, g^3 = 1$. Show that G is finite.

Proof. Assume G is generated by two elements a, b, and any $g \in G$ has a representation $a^{\alpha_1}b^{\beta_1}a^{\alpha_2}b^{\beta_2}...$ or $b^{\beta_1}a^{\alpha_1}b^{\beta_2}a^{\alpha_2}...$ It suffices to prove any $g \in G$ has a representation with word length < 12.

If not, W.L.O.G., assume $g = a^{\alpha_1}b^{\beta_1}a^{\alpha_2}b^{\beta_2}...$ is a representation of g with minimal length ≥ 12, and $\alpha_i, \beta_i = \pm 1$.

If there exists $\alpha_i = \alpha_{i+1}$, then by $e = (a^{\alpha_i}b^{\beta_i})^3 = a^{\alpha_i}b^{\beta_i}a^{\alpha_i}b^{\beta_i}a^{\alpha_i}b^{\beta_i}$, we can substitute $a^{\alpha_i}b^{\beta_i}a^{\alpha_{i+1}}$ by $b^{-\beta_i}a^{-\alpha_i}b^{-\beta_i}$ to make the representation shorter. This contradicts the minimality assumption.

So $\alpha_i \neq \alpha_{i+1}$ for any i and for the same reason $\beta_i \neq \beta_{i+1}$ for any i. So $g = a^{\alpha_1}b^{\beta_1}a^{-\alpha_1}b^{-\beta_1}a^{\alpha_1}b^{\beta_1}a^{-\alpha_1}b^{-\beta_1}a^{\alpha_1}b^{\beta_1}a^{-\alpha_1}b^{-\beta_1}...$ Then we can substitute the beginning

$$a^{\alpha_1}b^{\beta_1}a^{-\alpha_1}b^{-\beta_1}a^{\alpha_1}b^{\beta_1}a^{-\alpha_1}b^{-\beta_1}a^{\alpha_1}b^{\beta_1}a^{-\alpha_1}b^{-\beta_1} = (a^{\alpha_1}b^{\beta_1}a^{-\alpha_1}b^{-\beta_1})^3$$

by 1 to make the representation shorter. This is also contradictory. □