ALGEBRA: HOMEWORK 4

Problem 1. Find a normal subgroup of symmetric group $\mathcal{S}_4$ of order 4.

Proof. In last homework we have known that there are 3 subgroup of $\mathcal{S}_4$ of order 8:

$$\begin{aligned} G_1 =& \{id, (12)(34), (23)(14), (13)(23), (13), (14), (1234), (4321)\} \\ G_2 =& \{id, (12)(34), (23)(14), (13)(23), (12), (34), (1324), (4231)\} \\ G_3 =& \{id, (12)(34), (23)(14), (13)(23), (14), (23), (1243), (3421)\}. \end{aligned}$$

By Sylow's theorem, any subgroup of order 4 must be contained in one of G_1, G_2, G_3, and G_1, G_2, G_3 are conjugated to each other. Assume N is a normal subgroup of order 4 and $N \subset G_1$, and $gG_1g^{-1} = G_2, hG_1h^{-1}G_3$. Then $N = gNg^{-1} \subset G_2$, $N = hNh^{-1} \subset G_3$. Then

$$N \subset G_1 \cap G_2 \cap G_3 = \{id, (12)(34), (23)(14), (13)(23)\}.$$

So N must be $\{id, (12)(34), (23)(14), (13)(23)\}$.

Now we prove $N = \{id, (12)(34), (23)(14), (13)(23)\}$ is a normal subgroup. Since the intersection of subgroups is still a subgroup, so N is clearly a subgroup. For any $g \in G$, the g-conjugation action on $\{G_1, G_2, G_3\}$ is bijective, so

$$\begin{aligned} gNg^{-1} =& g(G_1 \cap G_2 \cap G_3)g^{-1} \\ =& (gG_1g^{-1}) \cap (gG_3g^{-1}) \cap (gG_3g^{-1}) \\ =& G_1 \cap G_2 \cap G_3 = N \end{aligned}$$

and N is normal. □

Problem 2. Show that a group of order 385 is solvable.

Proof. Assume G is the group of order $385 = 5 \times 7 \times 11$ and by Sylow's theorem there exists subgroup of order 11. Assume n is the number of subgroups of order 11. By Sylow's theorem $n | 3 \times 5$ and $n = 1 \pmod{11}$, so $n = 1$ and there exists a normal subgroup H and the quotient group G/H is of order 5×7. Since $7 \neq 1$ (5), by a result in class we know that $G/H \cong C_{15}$ is abelian. So $\{e\} \lhd H \lhd G$ is a solvable chain. □

Problem 3. Write

$$(x^2 + y^2)(x^2 + z^2)(y^2 + z^2)$$

in terms of elementary symmetric functions $\sigma_1, \sigma_2, \sigma_3$.

Proof.

$$\begin{aligned}
&(x^2+y^2)(x^2+z^2)(y^2+z^2)\\
=&x^4y^2+x^4z^2+y^4x^2+y^4z^2+z^4x^2+z^4y^2+2x^2y^2z^2\\
=&(x^2+y^2+z^2)(x^2y^2+y^2z^2+z^2x^2)-x^2y^2z^2\\
=&(\sigma_1^2-2\sigma_2)(\sigma_2^2-2\sigma_1\sigma_3)-\sigma_3^2\\
=&\sigma_1^2\sigma_2^2-2\sigma_1^3\sigma_3-2\sigma_2^3+4\sigma_1\sigma_2\sigma_3-\sigma_3^2
\end{aligned}$$

□

Problem 4. Determine the ring of invariants $\mathbb{C}[x,y,z]^\Gamma$ for

$$\Gamma := \left\{ \begin{pmatrix} \pm1 & 0 & 0 \\ 0 & \pm1 & 0 \\ 0 & 0 & \pm1 \end{pmatrix} \right\} \subset GL_3(\mathbb{C}).$$

Proof. Assume $f(x,y,z) = \sum a_{ijk}x^iy^jz^k \subset \mathbb{C}[x,y,z]^\Gamma$. Then by $f(x,y,z) = f(-x,y,z)$, we have $\sum a_{ijk}x^iy^jz^k \equiv \sum(-1)^i a_{ijk}x^iy^jz^k$, i.e., $a_{ijk} = (-1)^i a_{ijk}$. So for odd i, $a_{ijk} = 0$ and for the same reason $a_{ijk} = 0$ if j or k is odd. So f have the form $f = \sum b_{ijk}x^{2i}y^{2j}z^{2k} \in \mathbb{C}[x^2,y^2,z^2]$. So $\mathbb{C}[x,y,z]^\Gamma \subset \mathbb{C}[x^2,y^2,z^2]$, and it is easy to verify $\mathbb{C}[x^2,y^2,z^2] \subset \mathbb{C}[x,y,z]^\Gamma$. So $\mathbb{C}[x,y,z]^\Gamma = \mathbb{C}[x^2,y^2,z^2]$.

□

Problem 5. Find generators of the ring of invariants $\mathbb{F}_2[x,y,z]^\Gamma$ for

$$\Gamma := \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\} \subset GL_3(\mathbb{F}_2),$$

where $*$ is 0 or 1, i.e., Γ is the Heisenberg group over $\mathbb{F}_2$.

Proof. We claim that $x(x+y)(x+z)(x+y+z), y(y+z), z$ are generators of $\mathbb{F}_2[x,y,z]^\Gamma$.

It is easy to check that these three polynomials are invariant under Γ and now we prove that any $f \in \mathbb{F}_2[x,y,z]^\Gamma$ is a polynomial of there three.

Assume $f = \sum a_{ijk}x^iy^jz^k \in \mathbb{F}_2[x,y,z]^\Gamma$. Use the lexicographical order defined in class and assume $x^py^qz^r$ is the leading term of f.

(1) If $p > 0$,

expand both sides in $f(x+y,y,z) \equiv f(x,y,z)$ and compare the coefficients of $x^{p-1}y^{q+1}z^r$, we have $2|p$;

expand both sides of $f(x,y+z,z) \equiv f(x,y,z)$ and compare the coefficients of $x^py^{q-1}z^{r+1}$, we have $2|q$;

expand both sides in $f(x+y, y, z) \equiv f(x, y, z)$ and compare the coefficients of $x^{p-2}y^{q+2}z^r$, we have that the coefficient of $x^{p-1}y^{q+1}z^r$ in f is equal to $C_p^2 = p(p-1)/2 \bmod (2)$.

expand both sides in $f(x, y+z, z) \equiv f(x, y, z)$ and compare the coefficients of $x^{p-1}y^q z^{r+1}$, we have that the coefficient of $x^{p-1}y^{q+1}z^r$ in f is even, i.e., $C_p^2 = p(p-1)/2$ is even. So $4|p$.

(2) If $p = 0$, expand both sides of $f(x, y+z, z) \equiv f(x, y, z)$ and compare the coefficients of $y^{q-1}z^{r+1}$, we have $2|q$.

Now we prove by induction on the leading term of f. If $p > 0$, $f - [x(x+y)(x+z)(x+y+z)]^{p/4}$ is invariant and has strictly smaller leading term; if $p = 0, q \neq 0$, $f - [y(y+z)]^{q/2}$ has strictly smaller leading term; if $p = q = 0$, then f is a polynomial of z. □