(worked with Joseph Sullivan)

1 Exercise I.13

(a) Let H, N be normal subgroups of a finite group G. Assume that the orders of H, N are relatively prime. Prove that $xy = yx$ for all $x \in H$ and $y \in N$, and that $H \times N \cong HN$.

Proof. Since $H \cap N$ is a subgroup of both H and N, its order divides $\gcd(|H|, |N|) = 1$, so it must be the trivial subgroup. Hence, we have an isomorphism

$$\begin{aligned} H \xrightarrow{\sim} H/(H \cap N) &\xrightarrow{\sim} HN/N, \\ x \longmapsto\quad &\quad xN. \end{aligned}$$

Given $x \in H$ and $y \in N$, we have $yxy^{-1} \in H$, since H is normal. This map sends yxy^{-1} to

$$yxy^{-1}N = yxN = yNx = Nx = xN,$$

which is also the image of x. Since this is an isomorphism, we conclude that $yxy^{-1} = x$, or, equivalently, that $xy = yx$.

By Proposition 2.1 in Lang, the map

$$\begin{aligned} H \times N &\longrightarrow HN, \\ (x, y) &\longmapsto xy, \end{aligned}$$

is a group isomorphism. □

(b) Let $H_1, \dots, H_r$ be normal subgroups of G such that the order of H_i is relatively prime to the order of H_j for $i \neq j$. Prove that

$$H_1 \times \cdots \times H_r \cong H_1 \cdots H_r.$$

Proof. We perform induction on r. The result is trivial for $r = 1$.

Assume that the result holds for any $r - 1$ normal subgroups with mutually relatively prime orders, so $H_1 \times \cdots \times H_{r-1} \cong H_1 \cdots H_{r-1}$. Then $H_1 \cdots H_{r-1}$ is a normal subgroup of G with order $|H_1| \cdots |H_{r-1}|$, which is relatively prime to $|H_r|$. Applying the inductive hypothesis, followed by part (a), we deduce

$$(H_1 \times \cdots \times H_{r-1}) \times H_r \cong (H_1 \cdots H_{r-1}) \times H_r \cong H_1 \cdots H_{r-1} H_r.$$

□

2 Exercise I.20 Let P be a p-group. Let A be a normal subgroup of order p. Prove that A is contained in the center of P.

Proof. Since the order of A is prime, it is cyclic; say $A = \langle x \rangle \cong \mathbb{Z}/p\mathbb{Z}$. The fact that A is normal implies $yxy^{-1} \in A$, for all $y \in P$. In particular, $yxy^{-1} = x^k$ with $0 < k < p$. So, we can define a group homomorphism $\alpha : P \to (\mathbb{Z}/p\mathbb{Z})^\times$ such that $yxy^{-1} = x^{\alpha(y)}$, for all $y \in P$. Then $\operatorname{im}\alpha$ is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$, so its order divides $p-1$. On the other hand, $|\operatorname{im}\alpha| = [P : \ker\alpha]$ divides $|P|$, so $|\operatorname{im}\alpha|$ must be a power of p. Therefore, $\operatorname{im}\alpha$ must be trivial, implying $yxy^{-1} = x^{\alpha(y)} = x^1$. Since the generator of A commutes with every element of P, so does every other element of A, hence $A \subseteq Z(P)$.

$\square$

3 Exercise I.32 Let S_n be the permutation group on n elements. Determine the p-Sylow subgroups of S_3, S_4, S_5 for $p = 2$ and $p = 3$.

$\mathbf{S_3}$ We have $n_2 \equiv 1 \pmod 2$ and $n_2 \mid 3$, implying that $n_2 \in \{1, 3\}$. There are at least three distinct Sylow 2-subgroups:

$$\langle (1\ 2) \rangle, \quad \langle (1\ 3) \rangle, \quad \langle (2\ 3) \rangle.$$

Therefore, $n_2 = 3$, and these are the only Sylow 2-subgroups.

We have $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 2$, implying that $n_3 = 1$. The unique Sylow 3-subgroup is

$$\langle (1\ 2\ 3) \rangle.$$

$\mathbf{S_4}$ We have $n_2 \equiv 1 \pmod 2$ and $n_2 \mid 3$, implying that $n_2 \in \{1, 3\}$. We can embed the dihedral group

$$D_8 = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$$

into S_4 in three distinct ways (arising from labeling the vertices of a square):

$$\sigma = (1\ 2\ 3\ 4), \tau = (2\ 4); \quad \sigma = (1\ 2\ 4\ 3), \tau = (2\ 3); \quad \sigma = (1\ 3\ 2\ 4), \tau = (3\ 4).$$

Therefore, $n_2 = 3$, and these are the only Sylow 2-subgroups.

We have $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 8$, implying that $n_3 \in \{1, 4\}$. We can embed the cyclic group

$$\mathbb{Z}/3\mathbb{Z} \cong \langle \alpha \mid \alpha^3 = 1 \rangle$$

into S_4 in four distinct ways:

$$\alpha = (1\ 2\ 3), \quad \alpha = (1\ 2\ 4), \quad \alpha = (1\ 3\ 4), \quad \alpha = (2\ 3\ 4).$$

Therefore, $n_3 = 4$, and these are the only Sylow 3-subgroups.

$\mathbf{S_5}$ We have $n_2 \equiv 1 \pmod 2$ and $n_2 \mid 15$, implying that $n_2 \in \{1, 3, 5, 15\}$. We can embed the symmetric group S_4 into S_5 in five distinct ways: one being the natural inclusion (i.e., treating every permutation of four elements as a permutation of five elements, always fixing the fifth), and the other four being obtained by replacing any occurrence of some chosen index (1, 2, 3, or 4) with 5 in each permutation. From our previous analysis, we know that D_8 can be embedded into S_4 in three ways, and composing with the five embeddings of S_4 into S_5, we obtain fifteen distinct embeddings of D_8 into S_5. (The fact that all fifteen are distinct can be seen from the fact that each embedding of D_8 into S_4 utilizes all four indices, and each embedding of S_4 differs by exactly one index.) Therefore, $n_2 = 15$, and these are the only Sylow 2-subgroups.

We have $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 40$, implying that $n_3 \in \{1, 4, 10\}$. We can embed the cyclic group $\mathbb{Z}/3\mathbb{Z}$ into S_5 in $\binom{5}{3} = 10$ distinct ways:

$$\alpha = (i\ j\ k), \text{ for each choice of } \{i, j, k\} \subseteq \{1, 2, 3, 4, 5\}.$$

(One can check that these can also be obtained by composing embeddings of the cyclic group into S_4, then S_4 into S_5, but that there will be overlap.) Therefore, $n_3 = 10$, and these are the only Sylow 3-subgroups.

4 Exercise I.55 Let $M \in \mathrm{GL}_2(\mathbb{C})$. We let

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \text{ and for } z \in \mathbb{C} \text{ we let } M(z) = \frac{az+b}{cz+d}.$$

If $z = -d/c$ ($c \neq 0$) then we put $M(z) = \infty$. Then you can verify that $\mathrm{GL}_2(\mathbb{C})$ thus operates on $\mathbb{C} \cup \{\infty\}$. Let λ, λ' be the eigenvalues of M viewed as a linear map on $\mathbb{C}^2$. Let W, W' be the corresponding eigenvectors,

$$W = \begin{bmatrix} w_1 & w_2 \end{bmatrix}^T \quad \text{and} \quad W' = \begin{bmatrix} w_1' & w_2' \end{bmatrix}^T.$$

Assume that M has two distinct fixed points $\neq \infty$.

(a) Show that there cannot be more than two fixed points and that these fixed points are $w = w_1/w_2$ and $w' = w_1'/w_2'$. In fact one may take

$$W = \begin{bmatrix} w & 1 \end{bmatrix}^T, \quad W' = \begin{bmatrix} w' & 1 \end{bmatrix}^T.$$

Proof. If w is a fixed point of M, $w = (aw+b)/(cw+d)$ implies w is a root of the complex polynomial

$$cz^2 + (d-a)z + b = 0.$$

Since a complex quadratic has to most two distinct complex roots, M has at most two distinct fixed points.

We now check that w_1/w_2 is a fixed point of M:

$$M(w_1/w_2) = \frac{aw_1/w_2 + b}{cw_1/w_2 + d} = \frac{aw_1 + bw_2}{cw_1 + dw_2} = \frac{(MW)_1}{(MW)_2} = \frac{(\lambda W)_1}{(\lambda W)_2} = \frac{\lambda w_1}{\lambda w_2} = \frac{w_1}{w_2}.$$

The same is true of w_1'/w_2'.

By linearity, any nonzero scalar of an eigenvector is, again, an eigenvector with the same eigenvalue. So $\frac{1}{w_2}W = \begin{bmatrix} w & 1 \end{bmatrix}^T$ and $\frac{1}{w_2'}W' = \begin{bmatrix} w' & 1 \end{bmatrix}^T$ are eigenvectors for λ and λ', respectively.

$\square$

(b) Assume that $|\lambda| < |\lambda'|$. Given $z \neq w$, show that

$$\lim_{k\to\infty} M^k(z) = w'.$$

[*Hint*: Let $S = \begin{bmatrix} W & W' \end{bmatrix}$ and consider $S^{-1}M^kS(z) = \alpha^k z$ where $\alpha = \lambda/\lambda'$.]

Proof. We compute

$$\begin{aligned}
S^{-1}MS &= S^{-1}M \begin{bmatrix} W & W' \end{bmatrix} \\
&= S^{-1} \begin{bmatrix} \lambda W & \lambda' W' \end{bmatrix} \\
&= S^{-1} \begin{bmatrix} \lambda w & \lambda' w' \\ \lambda & \lambda' \end{bmatrix} \\
&= S^{-1}S \begin{bmatrix} \lambda & 0 \\ 0 & \lambda' \end{bmatrix} \\
&= \begin{bmatrix} \lambda & 0 \\ 0 & \lambda' \end{bmatrix},
\end{aligned}$$

so

$$S^{-1}M^kS = (S^{-1}MS)^k = \begin{bmatrix} \lambda^k & 0 \\ 0 & (\lambda')^k \end{bmatrix}.$$

Thus, as per the hint, $S^{-1}M^kS(z) = \alpha^k z$ where $\alpha = \lambda/\lambda'$. Since $0 \leq \alpha < 1$, we have the limit $a^k z \to 0$. Note that fractional linear transformations are bicontinuous, so

$$\begin{aligned}
\lim_{k\to\infty} M^k(z) &= SS^{-1}\left(\lim_{k\to\infty} M^k(SS^{-1}(z))\right) \\
&= S\left(\lim_{k\to\infty} S^{-1}M^kS(S^{-1}(z))\right) \\
&= S\left(\lim_{k\to\infty} \alpha^k S^{-1}(z)\right) \\
&= S(0) \\
&= \frac{w \cdot 0 + w'}{1 \cdot 0 + 1} \\
&= w'.
\end{aligned}$$

(Note that $S^{-1}(z)$ contains $w - z$ in its denominator, so we require that $z \neq w$ for the third step to make sense.)

$\square$