# Exercises from Ch. 1: Groups, Lang

Matthew Gergley

Last Updated: January 9, 2026

## Exercises

**Exercise 0.1.** (Exercise 1) Show that every group of order $\leq 5$ is abelian.

*Proof.* First, we will take care of the cases where $|G|$ is prime (i.e. 2, 3, 5). We prove this by showing that the groups of these orders are cyclic and thus abelian (cyclic $\Rightarrow$ abelian). Suppose that $|G| = p \leq 5$, a prime. Then, by Lagrange's Theorem, for all $x \in G$, $|x| \bigm| |G|$. Hence, $|x| \bigm| p$. Therefore, $|x| = 1$ or $|x| = p$. If $|x| = 1$, then $x = e$ and we get $|G| = 1$ which is not a prime, but is also trivially abelian. If $|x| = p$, then let $G = \langle x \rangle$. Thus, $G = \{e = x^{|G|},\, x,\, x \cdot x = x^2\,, x \cdot x \cdot x = x^3, \, \ldots\,, x^{|G|-1}\}$. Clearly, $G$ is abelian since $x \cdot x^j = x^j \cdot x$ for all $x \in G$ and $1 \leq j \leq |G|$. Thus, if $|G| \leq 5$ is prime, then $G$ is abelian. Next suppose $|G| = 4 = 2^2$. We prove a general case that all groups of order $p^2$ for a prime $p$ are abelian and thus it would follow that $G$ is abelian if $|G| = 4$.
Suppose $|G| = p^2$ for a prime $p$. Hence, $G$ is a $p - group$ and hence $Z(G)$ is not trivial. Recall that the class equation is defined as

$$|G| = |Z(G)| + \sum_{x \in C} (G\colon G_x)$$

where $C$ is a set of representatives for the distinct conjugacy classes and $G_x$ is the isotropy group of $x$ in $G$ defined by $G_x = \{y \in G : \; x \cdot y = y\}$. But here we can consider $G$ acting on itself by conjugation and thus $G_x = \{y \in G : \; yxy^{-1} = x\} = C_G(x) = \{g \in G : \; gx = xg\}$. Each term in $\sum\limits_{x \in C}(G\colon G_x) > 1$ and divides $|G| = p^2$. Hence, $\sum\limits_{x \in C}(G\colon G_x) \equiv 0 \pmod p$. Therefore, $|G| = |Z(G)| + kp$ ($k \in \mathbb{Z}^+$, and $kp = \sum(G\colon G_x)$). Then, $|Z(G)| = |G| - kp \Rightarrow |Z(G)| \equiv 0 \pmod p$. Thus, $p \bigm| |Z(G)| \Rightarrow |Z(G)| = p$ or $p^2$ (since $|Z(G)| \leq |G|$).
<u>Case 1:</u> Suppose $|Z(G)| = p^2$. Then $|Z(G)| = |G| \Rightarrow Z(G) = G$. Thus, $G$ is abelian.
<u>Case 2:</u> Suppose $|Z(G)| = p$ Consider the quotient group $G/Z(G)$ (since $Z(G) \triangleleft G$). Thus, $|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p$. Hence, $G/Z(G)$ is cyclic by above and thus $G/Z(G)$ is abelian. Now we will show that the fact that $G/Z(G)$ is abelian implies that $G$ is abelian.
Since $G/Z(G)$ is cyclic, $G/Z(G) = \langle gZ(G) \rangle$. Thus, $xZ(G) = (gZ(G))^k = g^k Z(G)$ for some $k \in \mathbb{Z}$. By coset equality, $xZ(G) = g^k Z(G) \iff x(g^k)^{-1} \in Z(G) \iff x = g^k z_1$ for some $z_1 \in Z(G)$. Hence, every element of $x \in G$ can be written as $x = g^k z_1$ for some $k \in \mathbb{Z}$ and $z_1 \in Z(G)$. Similarly, let $y \in G$ and thus $y = g^\ell z_2$ for some $\ell \in \mathbb{Z}$ and $z_2 \in Z(G)$. We want to show that $xy = yx$. Then,

$$xy = g^k z_1 g^\ell z_2 = g^{k+\ell} z_1 z_2 = g^{\ell+k} z_2 z_1 = g^\ell z_2 g^k z_1 = yx$$

Therefore, $G$ is abelian and note that we were able to commute elements since $z_1, z_2 \in Z(G)$. Thus, we have shown that if $G/Z(G)$ is cyclic, then $G$ is abelian. We are done.

$\square$

**Exercise 0.2.** (Exercise 7) Let $G$ be a group such that $Aut(G)$ is cyclic. Prove that $G$ is abelian.

*Proof.* Suppose $Aut(G)$ is cyclic. Hence, $Inn(G)$ is cyclic since $Inn(G) \subseteq Aut(G)$. Consider the map $\psi : G \to Inn(G)$ given by $g \mapsto \phi_g$ for all $g \in G$ where $\phi_g : G \to G$ by $x \mapsto gxg^{-1}$ for all $x \in G$. Notice that $\operatorname{Ker}\psi = Z(G)$, since if $\phi_g(x) = gxg^{-1} = x$, then $gx = xg \Rightarrow g \in Z(G)$. Thus, by the 1st Isomorphism Theorem, $G/\operatorname{Ker}\psi \cong Inn(G) \Rightarrow G/Z(G) \cong Inn(G)$. Since we have this isomorphism, $G/Z(G)$ and $Inn(G)$ have the same group structure, i.e. $G/Z(G)$ is cyclic and thus $G/Z(G)$ is abelian which implies from **Exercise 1** that $G$ is abelian.

$\square$

**Exercise 0.3.** (Exercise 10) Let $G$ be a group and let $H$ be a subgroup of finite index. Prove that there is only a finite number of right cosets of $H$, and that the number of right cosets is equal to the number of left cosets.

*Proof.* By assumption, $(G\colon H) = n < \infty$. The group $G$ acts on $G/H$ in two ways:

$$\lambda\colon G \to \mathrm{Perm}(G/H)$$

by $x \mapsto x(gH)$ for some $g \in G$ and

$$\rho\colon G \to \mathrm{Perm}(G/H)$$

by $x \mapsto (gH)x$ for some $g \in G$. Consider the coset $eH = H \in G/H$. The isotropy group of $eH$ in $G$ under $\lambda$ is

$$G^{\lambda}_{eH} = \{g \in G : \ g(eH) = eH = H\} = H.$$

The orbit of $eH$ under $G$ via $\lambda$ is

$$(G \cdot (eH))^{\lambda} = \{g(eH) : \ g \in G\} = G/H.$$

By the orbit-stabilizer theorem and Lagrange's theorem,

$$|(G \cdot (eH))^{\lambda}| = |G/H| = (G\colon G^{\lambda}_{eH}) = (G\colon H) = n < \infty.$$

Under $\rho$, we have the stabilizer of $eH$ in $G$ given by

$$G^{\rho}_{eH} = \{g \in G : \ (eH)g = eH = H\},$$

i.e. elements of $g$ such that $Hg = H$. If $Hg = H$, then $g = eg \in Hg = H$ and thus $g \in H$. Then clearly, $Hg \subseteq H$ and $g^{-1} \in H$ gives $H \subseteq Hg$, so $H = Hg$. Therefore, $G^{\rho}_{eH} = H$. The orbit of $eH$ under $\rho$ in $G$ is

$$(G \cdot (eH))^{\rho} = \{(eH)g : \ g \in G\} = Hg = H/G$$

Again, by the orbit-stabilizer theorem and Lagrange's,

$$|G \cdot (eH)| = |H \setminus G| = (G\colon G^{\rho}_{eH}) = (G\colon H) = n < \infty.$$

Therefore, $|H \setminus G| = |G/H| = n < \infty$, i.e. there is a finite number of right cosets, denoted by $H \setminus G$ (recall $H \leq G$), and the number of left cosets is the same as the number of right cosets.

□

**Exercise 0.4.** (Exercise 10) Let $G$ be a group and let $H$ be a subgroup of finite index. Prove that there is only a finite number of right cosets of $H$, and that the number of right cosets is equal to the number of left cosets.

*Proof.* By assumption, $(G\colon H) = n < \infty$. The group $G$ acts on $G/H$ in two ways:

$$\lambda : G \to \mathrm{Perm}(G/H)$$

by $x \mapsto x(gH)$ for some $g \in G$ and

$$\rho : G \to \mathrm{Perm}(G/H)$$

by $x \mapsto (gH)x$ for some $g \in G$. Consider $eH = H \in G/H$. The isotropy group of $eH$ in $G$ is

$$G_{eH} = \{g \in G : \ g(eH) = eH = H\} = H.$$

The orbit of $eH$ under $G$ is

$$G \cdot eH = \{g(eH) : \ g \in G\} = G/H.$$

By the orbit-stabilizer theorem and Lagrange's Theorem,

$$|G/H| = |G \cdot eH| = \underbrace{(G\colon G_{eH})}_{\text{under } \lambda} = (G\colon H) = n < \infty.$$

Now, under $\rho$, $G_{eH} = \{g \in G:\ (eH)g = H\}$. If $Hg = H$, then $g = eg \in Hg = H$, so $g \in H$. Conversely, if $g \in G$, then clearly $Hg \subseteq H$ and $g^{-1} \in H$ gives $H \subseteq Hg$, so $H = Hg$. Hence, $G_{eH} = H$. The orbit of $eH$ under $\rho$ in $G$ is

$$G \cdot (eH) = \{(eH)g:\ g \in G\} = Hg = H/G \quad \text{(notation in Lang for right cosets)}$$

Again by the orbit-stabilizer theorem and Lagrange's

$$|H/G| = |G \cdot eH| = \underbrace{(G\colon G_{eH})}_{\text{under } \rho} = (G\colon H) = n < \infty.$$

Therefore, $|H/G| = |G/H| = n < \infty$, i.e. there is a finite number of right cosets and the number of left cosets is the same as the number of right cosets.

□

**Exercise 0.5.** (Exercise 11) Let $G$ be a group and $A$ a normal abelian subgroup. Show that $G/A$ operates on $A$ by conjugation, and in this manner get a homomorphism of $G/A$ into $Aut(A)$.

*Proof.* Define a map $\phi : G/A \to Aut(A)$ by $\phi(gA) = gAg^{-1}$ , $g \in G$. (Well-defined) Suppose that $gA = hA$. Then $h = ga \in H$ for some $a \in A$. For any $x \in A$, we have $hxh^{-1} = (ga)x(ga)^{-1} = g(axa^{-1})g^{-1}$. Since $A$ is abelian, $axa^{-1} = x$. Thus, $hxh^{-1} = gxg^{-1}$. Thus, the definition of $\phi$ does no depend on the choice of representative in $G/A$. ($\operatorname{Im}\phi \subseteq Aut(A)$) For each $g \in G$, the map $a \mapsto gag^{-1}$ is a homomorphism $A \to A$ since conjugation preserves products. It is bijective with inverse $a \mapsto g^{-1}ag$. Hence, $\phi(gA) \in Aut(A)$. (Homomorphism) For $gA, hA \in G/A$ and $x \in A$,

$$\begin{aligned}(\phi(gA) \circ \phi(hA))(x) &= g(hxh^{-1})g^{-1} \\ &= (gh)x(gh)^{-1} = \phi(ghA)(x).\end{aligned}$$

Therefore, $\phi$ is a group homomorphism. Thus, $G/A$ acts on $A$ by conjugation, and we obtain a homomorphism

$$\phi : G/A \to Aut(A)$$

Its kernel is $\operatorname{Ker}\phi = C_G(A)/A$, where $C_G(A)$ is the centralizer of $A$ in $G$.

□

**Exercise 0.6.** (Exercise 12) Let $G$ be a group and let $H, N$ be subgroups with $N$ normal. Let $\gamma_x$ be conjugation by an element $x \in G$.

a) Show that $x \mapsto \gamma_x$ induces a homomorphism $f : H \to Aut(N)$.

b) If $H \cap N = \{e\}$, show that the map $H \times N \to HN$ given by $(x, y) \mapsto xy$ is a bijection, and that this map is an isomorphism if and only if $f$ is trivial, i.e. $f(x) = id_N$ for all $x \in H$.

c) We define $G$ to be the **semidirect product** of $H$ and $N$ if $G = HN$ and $H \cap N = \{e\}$. Now, conversely, let $N, H$ be groups, and let $\psi : H \to Aut(N)$ be a given homomorphism. Construct a semidirect product as follows. Let $G$ be the set of pairs $(x, h)$ with $x \in N$, $h \in H$. Define the composition law

$$(x_1, h_1)(x_2, h_2) = (x_1\psi(h_1)x_2, h_1h_2)$$

Show that this is a group law, and yields a semidirect product of $N$ and $H$, identifying $N$ with the set of elements $(x, 1)$ and $H$ with the set of elements $(1, h)$.

*Proof.* a) First, let $e_H \in H$ be the identity element in $H$. Then, $f(e_H) = \gamma_{e_H}$. Let $n \in N$. Thus, $\gamma_{e_H}(n) = e_H n e_H^{-1} = n$ (since $N$ normal). Thus, $f(e_H) = \gamma_{e_H} = id_N$. It is also well-defined since if $h_1 = h_2$, then $f(h_1) = \gamma_{h_1}(n) = h_1 n h_1^{-1}$ and $f(h_2) = \gamma_{h_2}(n) = h_2 n h_2^{-1}$. Clearly, we then have $f(h_1) = f(h_2)$. Let $x, y \in H$. Then, $f(xy) = \gamma_{xy}$. Take $n \in N$, $\gamma_{xy}(n) = xyn(xy)^{-1} = xyny^{-1}x^{-1} = x(\gamma_y(n))x^{-1} = \gamma_x(\gamma_y(n)) = (\gamma_x \circ \gamma_y)(n) = f(x) \circ f(y)$ as desired.

b) (Well-defined) For any $h \in H$, $n \in N$, $hn \in HN = \{xy : x \in H, y \in N\}$. (Injective) Suppose $(x_1, y_1), (x_2, y_2) \in H \times N$ and suppose $\phi((x_1, y_1)) = \phi((x_2, y_2)) \Rightarrow x_1 y_1 = x_2 y_2 \Rightarrow x_2^{-1} x_1 = y_2 y_1^{-1}$. Note $x_2^{-1} x_1 \in H$ and $y_2 y_1^{-1} \in N$. Thus, $x_2^{-1} x_1 \in H \cap N$ and $y_2 y_1^{-1} \in H \cap N$. But $H \cap N = \{e\}$ by assumption, so $x_2^{-1} x_1 = e \Rightarrow x_1 = x_2$ and $y_2 y_1^{-1} = e \Rightarrow y_1 = y_2$. Hence, $(x_1, y_1) = (x_2, y_2)$. (Surjective) Let $z \in HN$. Then, $z = hn$ for some $h \in H$, $n \in N$. Hence, $\phi((h, n)) = hn = z$ with $(h, n)$ clearly an element of $H \times N$. Thus, $\phi : H \times N \to HN$ is a bijection.

**(**********************NEED TO DO SECOND PART STILL*************************)**

c) Let $\psi : H \to Aut(N)$ be given by $\psi(h) = \phi_h$ with $\phi_h(n) = n' \in N$. Thus, we define the composition of $(x_1, h_1), (x_2, h_2) \in N \times H$ by

$$\begin{aligned}(x_1, h_1)(x_2, h_2) &= (x_1 \psi(h_1)(x_2), h_1 h_2) \\ &= (x_1 \phi_{h_1}(x_2), h_1 h_2)\end{aligned}$$

(Identity) Let $e = (e_N, e_H) \in G = N \times H$. Then, $(x_1, h_1)(e_N, e_H) = (x_1 \psi(h_1)(e_N), h \cdot e_N) = (x_1 \phi_{h_1}(e_N), h_1) = (x_1 \cdot e_N, h_1) = (x_1, h_1)$ (since $\phi \in Aut(N)$ fixes the identity). Likewise, $(e_N, e_H)(x_1, h_1) = (x_1, h_1)$ and thus $e \in G$ which implies that $G \neq \varnothing$. (Closed) Observe that

$$\begin{aligned}(x_1, h_1)(x_2, h_2) &= (x_1 \psi(h_1)(x_2), h_1 h_2) \\ &= (x_1 \phi_{h_1}(x_2), h_1 h_2)\end{aligned}$$

and since $\phi_{h_1} \in Aut(N)$, $\phi_{h_1}(x_2) \in N$. Hence, $x_1 \phi_{h_1}(x_2) \in N$ and $h_1 h_2 \in H \Rightarrow (x_1 \phi_{h_1}(x_2), h_1 h_2) \in G = N \times H$. (Associativity) Let $(x_1, h_1), (x_2, h_2), (x_3, h_3) \in G$. Then,

$$\begin{aligned}(x_1, h_1)\left[(x_2, h_2)(x_3, h_3)\right] &= (x_1, h_1)(x_2 \psi(h_2)(x_3), h_2 h_3) \\ &= (x_1, h_1)(x_2 \phi_{h_2}(x_3), h_2 h_3) = (x_1 \psi(h_1)\left[x_2 \phi_{h_2}(x_3)\right], h_1 h_2 h_3) \\ &= (x_1 \phi_{h_1}(x_2 \phi_{h_2}(x_3)), h_1 h_2 h_3) \\ &= (x_1 \phi_{h_1}(x_2) \phi_{h_1}(\phi_{h_2}(x_3)), h_1 h_2 h_3)\end{aligned}$$

Now,

$$\begin{aligned}\left[(x_1, h_1)(x_2, h_2)\right](x_3, h_3) &= (x_1 \psi(h_1)(x_2), h_1 h_2)(x_3, h_3) \\ &= (x_1 \phi_{h_1}(x_2), h_1 h_2)(x_3, h_3) \\ &= (x_1 \phi_{h_1}(x_2) \psi(h_1 h_2)(x_3), h_1 h_2 h_3) \\ &= (x_1 \phi_{h_1}(x_2)(\psi(h_1)\psi(h_2))(x_3), h_1 h_2 h_3) \\ &= (x_1 \phi_{h_1}(x_2) \phi_{h_1}(\phi_{h_2}(x_3)), h_1 h_2 h_3)\end{aligned}$$

Thus, $(x_1, h_1)\left[(x_2, h_2)(x_3, h_3)\right] = \left[(x_1, h_1)(x_2, h_2)\right](x_3, h_3)$. (Inverses) Suppose that $(x_1, h_1)(x_2, h_2) = (e_N, e_H)$. Thus,

$$\begin{aligned}
(x_1,h_1)(x_2,h_2) &= (e_N,e_H)\\
\Rightarrow (x_1\psi(h_1)(x_2),h_1h_2) &= (e_N,e_H)\\
\Rightarrow (x_1\phi_{h_1}(x_2),h_1h_2) &= (e_N,e_H)\\
\Rightarrow x_1\phi_{h_1}(x_2) = e_N \quad &\text{and} \quad h_1h_2 = e_H\\
\Rightarrow \phi_{h_1}(x_2) = x_1^{-1} \qquad &\Rightarrow h_2 = h_1^{-1} \in H\\
\because\ \phi_{h_1} \in Aut(N), \phi_{h_1^{-1}} \in Aut(N)&\\
\Rightarrow \phi_{h_1^{-1}}(\phi_{h_1}(x_2)) = \phi_{h_1^{-1}}(x_1^{-1}) &\Rightarrow x_2 = \phi_{h_1^{-1}}(x_1^{-1}) \in N.
\end{aligned}$$

Therefore, $(x_1,h_1)^{-1} = (\phi_{h_1^{-1}}(x_1^{-1},h_1^{-1}) = (\psi(h_1^{-1})(x_1^{-1}),h_1^{-1}) \in G$. ($G = HN$) Let $(x,h) \in G = N \times H$. Then,

$$\begin{aligned}
(x,h) &= (x\phi_{e_H}(e_N), e_H \cdot h)\\
&= (x\psi(e_H)(e_N), e_H \cdot h)\\
&= \underbrace{(x,e_H)}_{\in N}\underbrace{(e_N,h)}_{\in H}
\end{aligned}$$

Thus, $G = NH$. ($N \cap H = \{e\}$) Note that $(x,e_H) \in H \iff x \in e_N$ and $(e_N,h) \in N \iff h = e_H$. Thus, $N \cap H = \{(e_N,e_H)\} = \{e\}$. Therefore,

$$G = N \rtimes_\psi H.$$

□

**Exercise 0.7.** (Exercise 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.* Assume $|A| = p$. Thus, $A \cong C_p$, the cyclic group of order $p$ (since prime order implies cyclic). Thus, $\mathrm{Aut}(A)$ is cyclic of order $p-1$. Define

$$\varphi : P \to \mathrm{Aut}(A)$$

by $g \mapsto c_g$, conjugation by $g$ in $A$. Since $A \lhd P$, and by previous exercises, $c_g$ is a bijective homomorphism of $A$ into itself, hence $c_g \in \mathrm{Aut}(A)$. Our map $\varphi$ is a homomorphism since for $g,h \in P$ we have

$$\varphi(gh) = c_{gh} = c_g \circ c_h = \varphi(g)\varphi(h).$$

By definition, $\varphi(P) \le \mathrm{Aut}(A)$, thus $|\varphi(P)| \Big| |\mathrm{Aut}(A)| \Rightarrow |\varphi(P)| \Big| p-1$. But $\varphi(P)$ is also a homomorphic image of the $p$-group $P$, hence $|\varphi(P)| = p^k$ for some $k$. This is due to the First Isomorphism Theorem which states

$$P/\ker\varphi \cong \varphi(P).$$

Since $|P| = p^n$ for some $n$ by assumption, and $\ker\varphi \le P$, by Lagrange's Theorem, $|\ker\varphi| = p^k$ for $k \le n$. Then, by counting sizes via the isomorphism,

$$|\varphi(P)| = |P/\ker\varphi| = \frac{|P|}{|\ker\varphi|} = \frac{p^n}{p^k} = p^{n-k} \quad \text{(a power of } p\text{)}$$

Whence, the only positive integer that is both a power of $p$ and a divisor $p-1$ is 1. Thus, $|\varphi(P)| = p^0 = 1$. Thus means $\varphi(P)$ is trivial, i.e. $\varphi(g) = \mathrm{id}_A$ for all $g \in P$. Then, $(\varphi(g))(a) = c_g(a) = gag^{-1} = a$ (since $\varphi(g)(a) = a$ by $\varphi(g) = \mathrm{id}_A$). Hence, $ga = ag$. Therefore every element of $A$ commutes with every element of $P$. Therefore,

$$A \subseteq Z(P).$$

□

**Exercise 0.8.** (Exercise 21) Let $G$ be a finite group and $H$ a subgroup. Let $P_H$ be a $p$-Sylow subgroup of $H$. Prove that there exists a $p$-Sylow subgroup $P$ of $G$ such that $P_H = P \cap H$.

*Proof.* Let $G$ be a finite group, $H \leq G$, and let $P_H$ be a $p$-Sylow subgroup of $H$. By Theorem 6.4, there exists a $p$-Sylow subgroup $P \leq G$ such that every $p$-subgroup of $G$ is contained in $P$. Hence, since $H \leq G$, $P_H$ is a $p$-subgroup of $G$ ($p$-Sylow subgroup of $H$, by assumption) and thus

$$P_H \subseteq P$$

Furthermore, $P_H \subseteq H \Rightarrow P_H \subseteq P \cap H$. Observe that $P \cap H \leq H$ and thus since $P$ is a $p$-subgroup (also Sylow), $P \cap H$ is a $p$-subgroup of $H$ and therefore $P \cap H \subseteq P_H$. Hence,

$$P \cap H = P_H.$$

$\square$

**Exercise 0.9.** (Exercise 23) Let $P, P'$ be $p$-Sylow subgroups of a finite group $G$.

a) If $P' \subseteq N(P)$ (normalizer of $P$), then $P' = P$.

b) If $N(P') = N(P)$, then $P' = P$.

c) We have $N(N(P)) = N(P)$.

*Proof.* a) Suppose $P' \subseteq N(P)$. Then, for all $x \in P'$, $xPx^{-1} = P$. Hence, $P \triangleleft P'$. But $|P| = |P'| = p^n$ with $p^n$ the highest power of $p$ dividing the order of $G$. Hence, $P = P'$.

b) We know $P' \subseteq N(P')$, $P \subseteq N(P)$. Thus, by assumption of $N(P') = N(P)$, we have $P' \subseteq N(P') = N(P)$, i.e. $P' \subseteq N(P)$. This is exactly the case for part (a), thus, it follows that $P' = P$.

c) ($N(P) \subseteq N(N(P))$) This follows trivially since, in general, for all $H \leqslant G$, $H \subseteq N(H)$ (i.e. the normalizer of a subgroup contains the subgroup, thus the normalizer of the normalizer contains the normalizer).

($N(N(P)) \subseteq N(P)$) Let $x \in N(P)$. Then, by definition, $xN(P)x^{-1} = N(P)$. By way of contradiction, suppose $x \notin N(P)$. Then, there exists some $p \in P$ such that $xpx^{-1} \notin P$. But $p \in P \subseteq N(P)$, so $xpx^{-1} \in xN(P)x^{-1} = N(P)$. This would imply $xpx^{-1} \in N(P) \setminus P$ do not all stabilize $P$ under conjugation, otherwise these elements would be in $N(P)$ which contradicts $x \notin N(P)$. Hence, $x \notin N(P)$ is impossible and therefore $N(N(P)) \subseteq N(P)$.

Therefore, $N(N(P)) = N(P)$.

$\square$

**Exercise 0.10.** (Exercise 24) Let $p$ be a prime number. Show that a group of order $p^2$ is abelian, and that there are only two such groups up to isomorphism.

*Proof.* Suppose $|G| = p^2$ for a prime $p$. Thus, $G$ is a $p$-group and hence $Z(G)$ is not trivial. Recall that the class equation is defined as

$$|G| = |Z(G)| + \sum_{x \in C} (G \colon G_x)$$

where $C$ is a set of representatives for the distinct conjugacy classes and $G_x$ is the isotropy group of $x$ in $G$ defined as $G_x = \{x \in G : xy = y\}$ with $y \in G$ (here $G$ is acting on itself via conjugation). Each term in $\sum\limits_{x \in C} (G \colon G_x) > 1$ and divides $|G| = p^2$. Hence, $\sum\limits_{x \in C} (G \colon G_x) \equiv 0 \pmod{p}$. Thus, $|G| = |Z(G)| + kp$ $(k \in \mathbb{Z}^+)$ $\left[kp = \sum\limits_{x \in C} (G \colon G_x)\right]$. Therefore, $|Z(G)| = |G| - kp \Rightarrow |Z(G)| \equiv 0 \pmod{p}$.
Thus, $p \,\big|\, |Z(G)| \Rightarrow |Z(G)| = p$ or $p^2$.
But by **Exercise 1**, Cases 1 and 2 cover this, thus, it follows that $G$ is abelian.
**NEED TO SHOW THE SECOND PART, i.e. two such groups up to isomorphism!!!!!!!!!!!** $\square$

**Exercise 0.11.** (Exercise 28) Let $p, q$ be distinct primes. Prove that a group of order $p^2q$ is solvable, and that one of its Sylow subgroups is normal.

*Proof.* Let $n_p$ and $n_q$ denote the number of $p$-Sylow and $q$-Sylow subgroups $G$, respectively. By Sylow's Theorems,

$$n_p \Big| q, \quad n_p \equiv 1 \pmod p, \quad n_q \Big| p^2, \quad n_q \equiv 1 \pmod q$$

Hence,

$$n_p \in \{1, q\}, \quad n_q \in \{1, p, p^2\}$$

Case 1: $(p < q)$ If $n_q = p$, then $q \Big| p - 1$ which is impossible since $q > p - 1$. If $n_q = p^2$, then $q \Big| (p-1)(p+1)$ which is impossible since $q > p + 1$ (as well). Thus, $n_q = 1$, so the $q$-Sylow subgroup $Q \triangleleft G$ is normal. Case 2: $(p > q)$ If $n_p = q$, then $p \Big| q - 1$ which is impossible since $p > q - 1$. Thus, $n_p = 1$, so the $p$-Sylow subgroups $P \triangleleft G$ is normal. In both cases, $G$ has a normal Sylow subgroup $N$ (either $|N| = q$ or $|N| = p^2$). Now consider the quotient $G/N$.

- $|N|$ is a prime power and therefore is solvable.
- $|G/N|$ is either $p^2$ or $pq$ and in either case, both are known to be solvable.

Since both $N$ and $G/N$ are solvable, it follows that $G$ is solvable. [The fact that $n_p, n_q = 1 \Rightarrow P, Q$ are normal is since all Sylow groups are conjugate and if there is only one Sylow subgroup, then it is fixed by conjugation by $G$, hence normal.]

□

**Exercise 0.12.** (Exercise 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 $p = 3$.

*Proof.* We utilize Thm 6.2 throughout the following derivations to justify existence. We will find the Sylow subgroups up to isomorphism. ($S_3$; order $3! = 6 = 2 \cdot 3$) Let $\mathbf{p} = \mathbf{2}$. The highest power of 2 dividing 6 is 2. Hence, let $P_2 \leqslant S_3$ be a 2-Sylow subgroups and hence $|P_2| = 2$. Thus, $P_2 \cong C_2$ ($P_2$ is the subgroup generated by any of the three transpositions of $S_3$). Let $\mathbf{p} = \mathbf{3}$. The highest power of 3 dividing 6 is 3. Hence, let $P_3 \leqslant S_3$ be a 3-Sylow subgroup, $|P_3| = 3$. Observe $(S_3 \colon P_3) = 2$, thus $P_3 \triangleleft S_3$ and the only nontrivial normal subgroup of $S_3$ is $A_3$. Hence, $P_3 = A_3 = \langle (123) \rangle \cong C_3$.
$S_4$; order $4! = 24 = 2^3 \cdot 3$ Let $\mathbf{p} = \mathbf{2}$. A 2-Sylow subgroup $P_2$ has order $2^3 = 8$. Note that all elements of a 2-Sylow subgroup have an order of a power of 2. For example:

- Transpositions have order 2.
- Product of disjoint transpositions have order 2.
- 4-cycles have order 4.

Thus, there are no 3-cycles. We will construct a 2-Sylow subgroup. Start with disjoint the disjoint transpositions $(12), (34)$. These cycles generate the Klein 4-group,

$$V_4 = \{(1), (12), (34), (12)(34)\}$$

Thus far, we have order 4. Now consider the permutation $(13)(24)$. Conjugation by this element yields,

$$(13)(24)(12)(13)(24) = (43) = (34)$$

Hence, $(13)(24)$ swaps the two generators of $V_4$. Now the subgroup

$$P_2 = \langle (12), (34), (13)(24) \rangle$$

contains $V_4$ as a normal subgroup and an element acting by symmetry. Furthermore, $|P_2| = 8$. A group of order 8 containing a normal Klein 4-subgroup, plus an element that swaps its generators, is exactly the Dihedral group, $D_4$. Hence,

$$P_2 \cong D_4$$

Thus, all 2-Sylow subgroups of $S_4$ are conjugate and isomorphic to $D_4$. Let $\mathbf{p} = \mathbf{3}$. A 3-Sylow subgroup of $S_4$ has order 3 and thus is generated by any 3-cycle. Thus, $P_3 \cong C_3$. $S_5$; order $5! = 120 = 2^3 \cdot 3 \cdot 5$ Since the 2-,3-Sylow subgroups of $S_5$ will have the same order as the 2-,3-Sylow subgroups of $S_4$, we have $P_2 \cong D_4$ and $P_3 \cong C_3$.

□

**Exercise 0.13.** (Exercise 55) Let $M \in \mathrm{GL}_2(\mathbb{C})$ ($2 \times 2$ complex matrices with non-zero determinant). We let

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

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

$$W = {}^t(w_1, w_2) \text{ and } W' = {}^t(w_1', w_2').$$

By a **fixed point** of $M$ on $\mathbb{C}$ we mean a complex number $z$ such that $M(z) = z$. 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

$$W = {}^t(w, 1),\ W' = {}^t(w', 1).$$

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

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

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

*Proof.* a) A point $z \in \mathbb{C}$ satisfies $M(z) = z$ if an only if

$$az + b = z(cz + d) \iff cz^2 + (d - a)z - b = 0$$

This is a quadratic in $z$. Hence $M$ has at most two finite ($\neq \infty$) fixed points. Suppose $c = 0$. Then $M(z) = (a/d)z + b/d$, and $M(z) = z$ reduces to a linear equation, yielding at most one finite fixed point (unless $M$ is a scalar multiple of the identity, in which case every point is fixed, but then $\lambda = \lambda'$, contradicting the existence of two distinct fixed points). Thus $c \neq 0$. Now consider the eigenvectors. Assume first that $w_2 = w_2' \neq 0$. Define

$$w \coloneqq w_1/w_2,\ w' = w_1'/w_2'.$$

The equation $MW = \lambda W$ implies

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w \\ 1 \end{pmatrix} = \lambda \begin{pmatrix} w \\ 1 \end{pmatrix}.$$

The second component gives $\lambda = cw + d$. Substituting into the first yields

$$aw + b = \lambda w = (cw + d)w \iff cw^2 + (d - a)w - b = 0$$

i.e. $M(w) = w$. Similarly, $M(w') = w'$. To justify $w_2 \neq 0$, suppose $w_2 = 0$. Then $W = {}^t(w_1, 0)$ with $w_1 \neq 0$ so

$$cw_1 = 0,\ dw_1 = \lambda w_1 \Rightarrow c = 0,\ \lambda = d.$$

But $c = 0$ implies at most one fixed point ($\neq \infty$), a contradiction. Thus $w_2 = w_2' \neq 0$. Rescaling gives the desired normalization.

b) Let $S = (W, W')$. Since $W, W'$ are eigenvectors for distinct eigenvalues, $S \in \mathrm{GL}_2(\mathbb{C})$ and

$$S^{-1}MS = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda' \end{pmatrix} =: \Lambda$$

Hence

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

Represent $z \in \mathbb{C}$ by the vector ${}^t(z, 1)$. Then

$$S^{-1} \begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$$

Applying $M^k$ in homogeneous coordinates gives

$$S^{-1}M^k \begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} \lambda^k \alpha_1 \\ (\lambda')^k \alpha_2 \end{pmatrix}.$$

Reconstructing the point:

$$M^k(z) = \frac{w\lambda^k \alpha_1 + w'(\lambda')^k \alpha_2}{\lambda^k \alpha_1 + (\lambda')^k \alpha_2}$$

Let $\alpha := \lambda/\lambda'$, so $|\alpha| < 1$. Then

$$M^k(z) = \frac{w\alpha^k \alpha_1 + w'\alpha_2}{\alpha^k \alpha_1 + \alpha_2}$$

As $k \to \infty$, $\alpha^k \to 0$, so

$$M^k(z) \to \frac{w'\alpha_2}{\alpha_2} = w',$$

provided $\alpha_2 \neq 0$. If $\alpha_2 = 0$, then

$$\begin{pmatrix} z \\ 1 \end{pmatrix} = \alpha_1 W \Rightarrow z = w.$$

Thus for $z \neq w$, the limit is $w'$ as claimed.

$\square$