2.5 The Lattice of Subgroups of a Group

9b) The divisors of 24 are $1, 2, 3, 4, 6, 8, 12$, and 24, so we have that the subgroup lattice of $\mathbb{Z}/24\mathbb{Z}$ is

$$\begin{tikzcd}
 & \langle 1\rangle & \\
\langle 3\rangle \arrow[ur] & & \langle 2\rangle \arrow[ul] \\
\langle 6\rangle \arrow[u] \arrow[urr] & & \langle 4\rangle \arrow[u] \\
\langle 12\rangle \arrow[u] \arrow[urr] & & \langle 8\rangle \arrow[u] \\
 & \langle 24\rangle \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

3.1 Definitions and Examples

1) Let $\phi : G \to H$ be a homomorphism and fix a subgroup $E \leq H$. Since $e' \in E$, we have $\phi(e) = e'$, thus $e \in \phi^{-1}(E)$. Now let $a, b \in \phi^{-1}(E)$, then $\phi(a), \phi(b) \in E$, and thus by the closure of E we have $\phi(a)\phi(b) = \phi(ab) \in E$, and thus $ab \in \phi^{-1}(E)$. We also have that $\phi(a)^{-1} = \phi(a^{-1}) \in E$, thus $a^{-1} \in \phi^{-1}(E)$, and thus $\phi^{-1}(E) \leq G$.

Now suppose $E \trianglelefteq H$. Let $h \in \phi^{-1}(E)$ and fix $g \in G$, then $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1}$. Since $\phi(h) \in E$ and $\phi(g) \in H$, we have that $\phi(ghg^{-1}) \in E$, thus $ghg^{-1} \in \phi^{-1}(E)$, which proves that $\phi^{-1}(E) \trianglelefteq G$.

Since $\{e'\} \trianglelefteq H$, we can deduce that $\phi^{-1}(\{e'\}) = \ker\phi \trianglelefteq G$. ■

6) Define $\phi : \mathbb{R}^\times \to \{\pm 1\}$ as $a \mapsto a/|a|$, then we have that $\phi^{-1}(\{1\}) = (0, \infty)$ and $\phi^{-1}(\{-1\}) = (-\infty, 0)$. Fix $a, b \in \mathbb{R}^\times$, then

$$\phi(ab) = \frac{ab}{|ab|} = \frac{a}{|a|} \cdot \frac{b}{|b|} = \phi(a)\phi(b),$$

thus ϕ is a homomorphism. ■

10) Fix $\overline{a}, \overline{b} \in \mathbb{Z}/8\mathbb{Z}$ with $\overline{a} = \overline{b}$, then $a \equiv b \pmod 8$, so we have that $a = b + 8n$ for some $n \in \mathbb{Z}$, but then $a = b + 4k$ with $k = 2n$, thus $a \equiv b \pmod 4$ and $\phi(\overline{a}) = \phi(\overline{b})$, showing that ϕ is well-defined. We also have that ϕ is surjective since $\overline{a}_8 \mapsto \overline{a}_4$ for $1 \leq a \leq 4$. Finally, we have that the fibers of ϕ are $\ker\phi = \phi^{-1}(\{\overline{1}\}) = \{\overline{1}, \overline{5}\}$, $\phi^{-1}(\{\overline{2}\}) = \{\overline{2}, \overline{6}\}$, $\phi^{-1}(\{\overline{3}\}) = \{\overline{3}, \overline{7}\}$, and $\phi^{-1}(\{\overline{4}\}) = \{\overline{4}, \overline{8}\}$.

24) Fix a group G and subgroups H and N where $N \trianglelefteq G$. Given $h \in H$ and $a \in H \cap N$, we have by closure that $hah^{-1} \in H$, and since $N \trianglelefteq G$ and $h \in G$, we have that $hah^{-1} \in N$, thus $hah^{-1} \in H \cap N$, and thus $H \cap N \trianglelefteq H$. ■

36) Let G be a group and suppose $G/Z(G)$ is cyclic, then $G/Z(G) = \langle aZ(G) \rangle$ for some $a \in G$. Fix $b_1, b_2 \in G$, then $b_1 Z(G) = a^m Z(G)$ and $b_2 Z(G) = a^n Z(G)$ for integers m and n, thus $b_1 b_2 Z(G) = a^m a^n Z(G) = a^{m+n} Z(G) = a^{n+m} Z(G) = a^n a^m Z(G) = b_2 b_1 Z(G)$, thus $b_1 b_2 = b_2 b_1$ and G is abelian. $\blacksquare$

40) Given a group G and a normal subgroup N of G, let $\overline{x}, \overline{y} \in G/N$ and suppose $\overline{xy} = \overline{yx}$, then $xyN = yxN$, thus $xyn_1 = yxn_2$ for some $n_1, n_2 \in N$. Consequently, $x^{-1}y^{-1}xy = n_2 n_1^{-1}$, thus $x^{-1}y^{-1}xy \in N$. Now, assume $x^{-1}y^{-1}xy \in N$ and fix $n_1 \in N$, then $x^{-1}y^{-1}xyn_1 = n_2$ for some $n_2 \in N$, thus $xyn_1 = yxn_2$ and $xyN \subseteq yxN$. We also have that $n_1^{-1}x^{-1}y^{-1} = n_2 y^{-1}x^{-1}$, for some $n_2 \in N$, and taking inverses we obtain $yxn_1 = xyn_2$, thus $yxN \subseteq xyN$, which shows that $xyN = yxN$ and thus $\overline{xy} = \overline{yx}$. $\blacksquare$

3.2 More on Cosets and Lagrange's Theorem

4) Let G be a group with $|G| = pq$ for primes p and q. Since $Z(G) \leq G$, we have that $|Z(G)| \in \{1, p, q, pq\}$. Clearly if $|Z(G)| = pq$ then $G = Z(G)$ and is abelian. If $|Z(G)| = 1$, then $Z(G) = \{e\}$ and we are finished. Now let $|Z(G)| = p$, then $|G/Z(G)| = |G| / |Z(G)| = pq/p = q$, and since q is prime we have that $G/Z(G)$ is cyclic, thus G is abelian. A similar argument shows that G is abelian if $|Z(G)| = q$. $\blacksquare$

8) Let H and K be finite subgroups of a group G where $(|H|, |K|) = 1$. We clearly have that $e \in H \cap K$. Now, suppose $x \in H$ has order > 1, then $|x|$ divides $|H|$, thus $(|x|, |K|) = 1$, and thus $x \notin K$. Note that the order of an element in a subgroup is equal to its order in the containing group. Similarly, we have that $(|y|, |H|) = 1$ for any non-identity element $y \in K$, thus $y \notin H$, thus $H \cap K = \{e\}$. $\blacksquare$

16) Fix $a \in \mathbb{Z}/p\mathbb{Z}$ and let $|a| = k$, then $a^k \equiv 1 \pmod{p}$. Since $\left|\left\langle a^k \right\rangle\right| = k$, we have by Lagrange's theorem that $k \mid p-1$, thus $p - 1 = kn$ for some $n \in \mathbb{Z}$. Thus we have that $a^p = a^{kn+1} = a^{kn}a = (a^k)^n a \equiv a \pmod{p}$. $\blacksquare$