Problem §1 (6.21) Find all groups of order 15.

Solution: Let G be a group of order 15. Then G has 3-Sylow subgroups and 5-Sylow subgroups. Inspecting the 5-Sylow subgroups, let k be the number of 5-Sylow subgroups of G. Sylow's theorem tells us that

$$k|15 \text{ and } k \equiv 1(\mod 5).$$

This thus forces $k = 1$; that is, G has a unique 5-Sylow subgroup, say H_5. H_5 is also normal, since for any $g \in G$ the conjugate subgroup $g^{-1}H_5 g$ is also a subgroup of order 5, and so equals H_5.

Next, Sylow's theorem also tells us that there exists at least one 3-Sylow subgroup, say H_3. From Remark 6.33, we have $H_3 \cap H_5 = \{e\}$, so we can write

$$H_3 = \{e, a, a^2\}, \ H_5 = \{e, b, b^2, b^3, b^4\}$$

(since all prime-order groups are cyclic); moreover, the only element in common is e.

Consider $aba^{-1} \in H_5$ (since H_5 is normal); then

$$aba^{-1} = b^j \text{ for some } 0 \leq j \leq 4.$$

We then get

$$\begin{aligned}
b &= a^{-1}b^j a \\
&= (a^{-1}ba)(a^{-1}ba)\dots(a^{-1}ba) \\
&= (a^{-1}ba)^j \\
&= (a^{-1}(a^{-1}b^j a)a)^j \\
&= (a^{-2}b^j a^2)^j \\
&= ((a^{-2}ba^2)\dots(a^{-2}ba^2))^j \\
&= (a^{-2}ba^2)^{j^2} \\
&= (a^{-3}b^j a^3)^{j^2} \\
&= eb^{j^3}e.
\end{aligned}$$

Thus $b = b^{j^3}$, so $b^{j^3-1} = e$. Since the order of b is 5, we need $j^3 - 1 \equiv 0 \mod 5$, or $j^3 \equiv 1 \mod 5$. Thus $j = 1$; so $a^{-1}ba = b$, or $ab = ba$. Since every element of G is a power of a times a power of b, G is thus Abelian. Moreover, the order of ab is 15:

$$\begin{aligned}
e = (ab)^k = a^k b^k &\implies a^k = b^{-k} \in H_3 \cap H_5 = \{e\} \\
&\implies a^k = b^k = e \\
&\implies 3|k \text{ and } 5|k \\
&\implies 15|k.
\end{aligned}$$

Hence any group G with 15 elements is a cyclic group of order 15.

Problem §2 (6.22) Let G be a finite group, and let H_1 and H_2 be normal subgroups having the property that $\gcd(|H_1|, |H_2|) = 1$. Prove that the elements of H_1 and H_2 commute with one another.

Solution: By Lagrange and since $H_1 \cap H_2$ is a subgroup of both H_1 and H_2, we have

$$|H_1 \cap H_2| \mid \gcd(|H_1|, |H_2|) = 1;$$

in other words, $H_1 \cap H_2 = \{e\}$.

Suppose $\alpha \in H_1, \ \beta \in H_2$. Since H_1 is normal, any $\alpha' \in H_1$ can be represented as $\alpha' = \beta^{-1}\alpha\beta$ for any $\beta \in H_2$; and similarly, any $\beta' \in H_2$ can be represented as $\beta' = \alpha\beta\alpha^{-1}$ for any $\alpha \in H_1$.

Consider $\alpha\beta\alpha^{-1}\beta^{-1} \in G$. Clearly,

$$\alpha(\beta\alpha^{-1}\beta^{-1}) = (\alpha\beta\alpha^{-1})\beta^{-1}.$$

Moreover,

$$\alpha(\beta\alpha^{-1}\beta^{-1}) = \alpha\alpha' \in H_1, \text{ where } \alpha' = \beta\alpha^{-1}\beta^{-1} \in H_1 \text{ (since } H_1 \text{ is normal)},$$

and

$$(\alpha\beta\alpha^{-1}\beta^{-1}) = \beta'\beta \in H_2, \text{ where } \beta' = \alpha\beta\alpha^{-1} \in H_2.$$

Thus

$$\alpha\beta\alpha^{-1}\beta^{-1} \in H_1 \cap H_2 = \{e\},$$

and so

$$\alpha\beta\alpha^{-1}\beta^{-1} = e \implies \alpha\beta = \beta\alpha.$$

Thus the elements of H_1 and H_2 commute with each other.

Problem §3 (6.23) Let G be a finite group of order pq, where p and q are primes satisfying $p > q$. Assume further that $p \not\equiv 1(\mod q)$.

(a) Prove that G is an Abelian group.

(b) Prove that G is cyclic.

Solution:

(a) By Sylow's Theorem, G has both a p-Sylow subgroup, say H_p, and a q-Sylow subgroup, say H_q. We first show that both subgroups are normal.

Clearly, $H_p \subseteq N_G(H_p)$, and $N_G(H_p) \subseteq G$ is a subgroup of G; by Lagrange, $|H_p| = p$ thus divides $|N_G(H_p)|$, and furthermore $|N_G(H_p)|$ divides $pq = |G|$. Thus $|N_G(H_p)|$ is an integer that divides pq and is divisible by p; so either

$$|N_G(H_p)| = p, \text{ or } |N_G(H_p)| = pq.$$

In the second case, $N_G(H_p) = G$, and so H_p is a normal subgroup and we are done. Otherwise, if $|N_G(H_p)| = p$, then $N_G(H_p) = H_p$, so from Theorem 6.35(c) we get

$$1 \equiv k = \frac{|G|}{|N_G(H_p)|} = \frac{pq}{p} = q \mod p.$$

But this implies $p \mid q - 1$, a contradiction of $p > q$. Thus H_p is a normal subgroup.

An analogous argument follows for H_q, except on the last step, we assume $p \not\equiv 1 \mod q$ to derive a contradiction, rather than relying on $p > q$.

Thus H_p and H_q are normal subgroups of G. Clearly, $\gcd(p, q) = 1$, and since both are normal subgroups, Problem 6.22 tells us that the elements of H_p and H_q commute with each other. However, since $p \cdot q = pq = |G|$, and Remark 6.33 shows us that $H_p \cap H_q = \{e\}$, every element in G can be formed by multiplying some element $a \in H_p$ and $b \in H_q$; that is, for every $g \in G$, $g = a \cdot b$ for some $a \in H_p$, $b \in H_q$. Precisely, since H_p and H_q are both groups of prime order, they are cyclic, say generated by some $a \in H_p$ and $b \in H_q$ respectively, and every element in G is a power of a times a power of b. Then for any $g, g' \in G$,

$$gg' = (a^i b^{i'})(a^j b^{j'}) = (a^i a^j)(b^{i'} b^{j'}) = (a^j a^i)(b^{j'} b^{i'}) = (a^j b^{j'})(a^i b^{i'}) = g'g.$$

Thus G is an Abelian group.

(b) Consider $ab \in G$ where $a \in H_p$ and $b \in H_q$ generate their subgroups respectively, and let k be some integer such that $(ab)^k = e$. Then

$$\begin{aligned}(ab)^k = a^k b^k = e &\implies a^k = b^{-k} \in H_p \cap H_q = \{e\}\\ &\implies a^k = b^k = e\\ &\implies p \mid k \text{ and } q \mid k\\ &\implies pq \mid k.\end{aligned}$$

Thus ab has order pq, and so G is a cyclic group.

Problem §4 (6.24) Let G be a group. An isomorphism from G to itself is called an *automorphism* of G. The set of automorphisms is denoted

$$\mathrm{Aut}(G) = \{\text{ group isomorphisms } G \to G\}.$$

We define a composition law on $\mathrm{Aut}(G)$ as follows: for $\alpha, \beta \in \mathrm{Aut}(G)$, $\alpha\beta$ is the map from G to G given by $(\alpha\beta)(g) = \alpha(\beta(g))$.

(a) Prove that this composition law makes G a group.

(b) Let $a \in G$. Define a map ϕ_a from G to G by

$$\phi_a : G \longrightarrow G,\ \phi_a(g) = aga^{-1}.$$

Prove that $\phi_a \in \mathrm{Aut}(G)$, and that the map

$$G \longrightarrow \mathrm{Aut}(G),\ a \longmapsto \phi_a,$$

is a group homomorphism.

(c) Prove that the kernel of the above homomorphism is the center $Z(G)$ of G.

(d) Elements of $\mathrm{Aut}(G)$ in the form ϕ_a, defined above for some $a \in G$, are called *inner automorphisms*, and all other elements of $\mathrm{Aut}(G)$ are called *outer automorphisms*. Prove that G is Abelian if and only if its only inner automorphism is the identity map.

(e) More generally, if H is a normal subgroup of G, prove that there is a well-defined group homomorphism

$$G \longrightarrow \mathrm{Aut}(H),\ a \longmapsto \phi_a, \quad \text{where } \phi_a(h) = aha^{-1},$$

and that the kernel of this homomorphism is the centralizer of H in G.

Solution:

(a) Compositions of isomorphisms give an isomorphism, so G is closed under composition. Moreover, function composition is associative. Clearly, the identity map

$$\phi_e : G \longrightarrow G,\ a \longmapsto a$$

is an isomorphism. Finally, a map is bijective if and only if it has an inverse; thus for any $\alpha \in \mathrm{Aut}(G)$, there exists some inverse isomorphism $\alpha^{-1} \in \mathrm{Aut}(G)$ such that

$$\alpha\alpha^{-1} = \alpha^{-1}\alpha = \phi_e.$$

Thus $\mathrm{Aut}(G)$ is a group under composition.

(b) We first show ϕ_a is a group homomorphism for any $a \in G$. Let $g, g' \in G$. Then

$$\phi_a(gg') = agg'a^{-1} = ageg'a^{-1} = ag(a^{-1}a)g'a^{-1} = (aga^{-1})(ag'a^{-1}) = \phi_a(g)\phi_a(g').$$

Now, let suppose $g_1, g_2 \in G$ and $\phi_a(g_1) = ag_1a^{-1} = ag_2a^{-1} = \phi_a(g_2)$. Then

$$ag_1a^{-1} = ag_2a^{-1} \iff a^{-1}ag_1a^{-1}a = a^{-1}ag_2a^{-1}a \iff g_1 = g_2.$$

Thus ϕ_a is injective.

Finally, for any $g \in G$, consider $a^{-1}ga \in G$ (since all of $a, a^{-1}, g \in G$). Then

$$\phi_a(a^{-1}ga) = a(a^{-1}ga)a^{-1} = g.$$

Thus ϕ_a is an isomorphism.

Let $\psi : G \to \mathrm{Aut}(G)$, where $\phi(a) = \phi_a$. Let $a_1, a_2 \in G$. For any $g \in G$,

$$\begin{aligned}\psi(a_1a_2)(g) = \phi_{a_1a_2}(g) &= a_1a_2ga_2^{-1}a_1^{-1}\\ &= a_1\phi_{a_2}(g)a_1^{-1} = \phi_{a_1} \circ \phi_{a_2}(g)\\ &= \psi(a_1)\psi(a_2)(g).\end{aligned}$$

Hence $\psi : G \to \mathrm{Aut}(G)$ is a group homomorphism.

(c) Recall that $\ker(\psi) = \{a \in G \mid \phi_a = \phi_e\}$; that is, ϕ_a must equal the identity isomorphism. Suppose $a \in \ker(\psi)$; then for any $g \in G$,

$$\phi_a(g) = aga^{-1} = g = \phi_e(g).$$

But then $ag = ga$; in other words, $a \in Z(G)$. Thus $\ker(\psi) = Z(G)$.

(d) Suppose G is Abelian. Then for any inner automorphism $\phi_a \in Aut(G)$,

$$\phi_a(g) = aga^{-1} = aa^{-1}g = g = \phi_e(g);$$

that is, any inner automorphism must be the identity map.

Conversely, suppose that the only inner automorphism is the identity map. Suppose G is not Abelian, and let $a \in G \setminus Z(G)$ be a non-trivial element in G that does not commute with every element in G. Then for some $g \in G$, $ag \neq ga$. From (b), we know $\phi_a \in \mathrm{Aut}(G)$; moreover,

$$\phi_a(g) = aga^{-1} \neq g = \phi_e(g).$$

Thus ϕ_a is a non-trivial inner automorphism; but this contradicts the only inner automorphism being the identity map. Thus G must be Abelian.

(e) Let $\varkappa : G \to \mathrm{Aut}(H)$, $\varkappa(a) = \phi_a$ with $\phi_a(h) = aha^{-1}$. To show well-definedness, we need that for every $a \in G$, $\phi_a \in \mathrm{Aut}(H)$. Indeed, this follows trivially from H being a normal subgroup, since $gHg^{-1} = H$ for any $g \in G$, so $ghg^{-1} \in H$; thus $\phi_a(H) = H$ and $\phi_a \in \mathrm{Aut}(H)$ for any $a \in G$, where an analogous argument from (b) can be used to show that ϕ_a is an isomorphism ($\varkappa$ is not necessarily well-defined if H is not normal, since we could have $\phi_a(h) = aha^{-1} \notin H$ for some $h \in H$). Consider $a_1, a_2 \in G$; then for any $h \in H$,

$$\varkappa(a_1a_2)(h) = a_1a_2ha_2^{-1}a_1^{-1} = a_1\varkappa(a_2)(h)a_1^{-1} = \varkappa(a_1)\varkappa(a_2)(h).$$

Thus $\varkappa$ is a well-defined group homomorphism. Any $a \in \ker(\varkappa)$ if $\phi_a(h) = aha^{-1} = h = \phi_e(h)$; this requires $ah = ha$, or equivalently, $a \in Z_G(H)$. Therefore $\ker(\varkappa) = Z_G(H)$.

Problem §5 (6.25) Let $\mathcal{C}_n$ be a cyclic subgroup of order n, and let $\mathrm{Aut}(\mathcal{C}_n)$ be the automorphism group of $\mathcal{C}_n$, as defined in Problem 6.24. Prove that $Aut(\mathcal{C}_n)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$, the unit group in the ring $\mathbb{Z}/n\mathbb{Z}$.

Solution: We begin with a lemma:

Lemma 1. *Let $\mathcal{C}_n$ be a cyclic group, with a generator $\langle g \rangle$. The order of any element $g^k \in \mathcal{C}_n$ is equal to $\frac{n}{\gcd(k,n)}$.*

Proof. We first show that $(g^k)^{\frac{n}{\gcd(k,n)}} = e$. Clearly,

$$(g^k)^{\frac{n}{\gcd(k,n)}} = (g^n)^{\frac{k}{\gcd(k,n)}} = e.$$

Then, we show that $\frac{n}{\gcd(k,n)}$ is the smallest positive integer α such that $(g^k)^\alpha = e$. Consider any m that satisfies $(g^k)^m = e$. Since $|g| = n$, we have $n \mid km$. This then gives

$$\frac{n}{\gcd(k,n)} \mid \frac{k}{\gcd(k,n)} m.$$

Note that, if we decompose $k = p_1 \cdot \ldots \cdot p_a$ and $n = q_1 \cdot \ldots \cdot q_b$ using the FToA and order them such that the first c primes $p_{0 \le i \le c} = q_i$ are equal and all $j > c$ have $p_j \neq q_j$, then $\gcd(k,n) = \prod_{i=0}^{c} p_i$, and $\gcd(\frac{n}{\gcd(k,n)}, \frac{k}{\gcd(k,n)}) = 1$ (since none of the leftover primes are the same).

In particular, this gives us

$$\frac{n}{\gcd(k,n)} \mid m,$$

since $\frac{n}{\gcd(k,n)}$ and $\frac{k}{\gcd(k,n)}$ are relatively prime, and thus do not affect each other's divisibility. Thus for any m such that $g^{km} = e$, we have $\frac{n}{\gcd(k,n)} \le m$, so the order of g^k is $\frac{n}{\gcd(k,n)}$. $\square$

Let g be a generator of $\mathcal{C}_n$, and consider the map

$$\varpi : (\mathbb{Z}/n\mathbb{Z})^* \to \mathrm{Aut}(\mathcal{C}_n),\ k \mod n \mapsto \psi_k,\ \text{where } \psi_k(g) = g^k.$$

We must first show that every ψ_k is an automorphism of $\mathcal{C}_n$. Recall that any isomorphism from $\mathcal{C}_n$ to $\mathcal{C}_n$ must preserve the orders of elements; in particular, they must map generators to generators (since generators determine the entire cyclic group). For $\psi_k(g) = g^k$, since $k \in (\mathbb{Z}/n\mathbb{Z})^*$, we have $\gcd(k,n) = 1$, so any generator g will still have order $\frac{n}{\gcd(k,n)} = n$ by Lemma 1.

We then show that ϖ is a group homomorphism. Let $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$, and recall that $ab \mod n \equiv (a \mod n)(b \mod n)$; then for any $g^i \in \mathcal{C}_n$,

$$\begin{aligned}
\varpi(ab)(g^i) &= \psi_{ab \mod n}(g^i) \\
&= (g^i)^{ab \mod n} \\
&= (g^i)^{(b \mod n)(a \mod n)} \\
&= \left((g^i)^{b \mod n}\right)^{a \mod n} \\
&= \varpi(b)(g^i)^{a \mod n} \\
&= \varpi(a)\varpi(b)(g^i).
\end{aligned}$$

Hence ϖ is a group homomorphism.

Suppose $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $\varpi(a)(g) = g^a = g^b = \varpi(b)(g)$ (we only inspect actions on g here, since $\psi_i(g)$ completely determines the image $\psi_i(\mathcal{C}_n)$). Since ψ_a and ψ_b are isomorphisms and thus maintain the order, we need

$$ak \equiv bk \mod n,$$

or equivalently $a \equiv b \mod n$. Thus ϖ is injective.

Consider any automorphism $\psi \in \mathrm{Aut}(\mathcal{C}_n)$. Recall again that ψ is an automorphism on $\mathcal{C}_n$ if and only if it preserves the orders of every element, in particular the generators of $\mathcal{C}_n$. Equivalently, any ψ must map $g \mapsto g^k$, where $\gcd(k,n) = 1$, since by Lemma 1, $|g| = \left|g^k\right| = n$ only if $\gcd(k,n) = 1$. But the set of all k that satisfy $\gcd(k,n) = 1$ is exactly and entirely the unit group $(\mathbb{Z}/n\mathbb{Z})^*$, by Proposition 3.17. Thus any automorphism ψ_k with $g \mapsto g^k$ has $k \in (\mathbb{Z}/n\mathbb{Z})^*$, and so ϖ is surjective.

Therefore ϖ is a group isomorphism, and so $\mathcal{C}_n \cong (\mathbb{Z}/n\mathbb{Z})^*$.