Solutions 04

1. Let G be a group. The ***commutator*** of the elements f and g in G is the element $[f, g] := f^{-1}g^{-1}fg$ in G. The ***commutator subgroup*** $G^{(1)}$ of G is the subgroup generated by all commutators; $G^{(1)} := \langle f^{-1}g^{-1}fg \mid f, g \in G\rangle$.

i. Prove that $G^{(1)}$ is a normal subgroup and the quotient group $G/G^{(1)}$ is abelian.

ii. Let $\pi \colon G \to G/G^{(1)}$ be the canonical group homomorphism. For any abelian group A, demonstrate that every group homomorphism $\varphi \colon G \to A$ factors as $\varphi = \varphi^{(1)} \circ \pi$ where $\varphi^{(1)} \colon G/G^{(1)} \to A/A^{(1)}$ is the induced group homomorphism.

iii. Show that a subgroup H of G contains $G^{(1)}$ if and only if H is normal and G/H is abelian.

Solution. Since $[f, g] := f^{-1}g^{-1}fg$ for any elements f and g in G, the elements f and g commute if and only if we have $[f, g] = e$.

i. Since $[f, g]^{-1} = (f^{-1}g^{-1}fg)^{-1} = g^{-1}f^{-1}gf = [g, f]$, each element of $G^{(1)}$ is a product of commutators. For any element h in G and any element $[f, g]$ in $G^{(1)}$, we have

$$\begin{aligned} h[f, g]h^{-1} &= hf^{-1}g^{-1}fgh^{-1} = hf^{-1}h^{-1}hg^{-1}h^{-1}hfh^{-1}hgh^{-1} \\ &= (hfh^{-1})^{-1}(hgh^{-1})^{-1}(hfh^{-1})(hgh^{-1}) = [hfh^{-1}, hgh^{-1}]\,, \end{aligned}$$

so $G^{(1)}$ is a normal subgroup of G. For any two cosets $f\,G^{(1)}$ and $h\,G^{(1)}$ in $G/G^{(1)}$, it follows that

$$\begin{aligned} [f\,G^{(1)}, h\,G^{(1)}] &= (f\,G^{(1)})^{-1}(h\,G^{(1)})^{-1}(f\,G^{(1)})(h\,G^{(1)}) \\ &= f^{-1}h^{-1}fh\,G^{(1)} = [f, h]\,G^{(1)} = G^{(1)}\,, \end{aligned}$$

so the quotient group $G/G^{(1)}$ is abelian.

ii. As A is any abelian group, we have $A^{(1)} = \langle e\rangle$, so $A/A^{(1)} = A$. Because the image under the group homomorphism φ of a commutator in group G is a commutator in abelian group A, we see that $\varphi(G^{(1)}) = \langle e\rangle = A^{(1)}$. The First Isomorphism Theorem shows that the induced map $\varphi^{(1)} \colon G/G^{(1)} \to A/A^{(1)} = A$, defined, for any element h in G, by $\varphi^{(1)}(h\,G^{(1)}) = \varphi(h)$, is a group homomorphism and $\varphi = \varphi^{(1)} \circ \pi$.

iii. Suppose that H is a subgroup of G containing the commutator subgroup $G^{(1)}$. Since $G/G^{(1)}$ is abelian, the quotient group $H/G^{(1)}$ is a normal subgroup of the quotient $G/G^{(1)}$. The Correspondence Theorem establishes that H is a normal subgroup of G. Hence, the Third Isomorphism Theorem demonstrates that $G/H \cong (G/G^{(1)})/(H/G^{(1)})$, so we conclude that G/H is also abelian.

Conversely, suppose that H is normal subgroup of G and the quotient G/H is abelian. For any elements f and g in G, we have $(f\,H)(g\,H) = (g\,H)(f\,H)$, which means $fg\,H = gf\,H$ and $g^{-1}f^{-1}gf = [g, f] \in H$. Therefore, we deduce that $G^{(1)} \subseteq H$. $\square$

2. Let $\langle m \rangle$ be the subgroup of integers $\mathbb{Z}$ generated by m and let $[r] := r\langle m \rangle$ denote the left coset in the quotient group $\mathbb{Z}/\langle m \rangle$ containing the integer r. Consider the set $(\mathbb{Z}/\langle m \rangle)^{\times} := \{\overline{r} \in \mathbb{Z}/\langle m \rangle \mid \gcd(r, m) = 1\}$.

i. Demonstrate that multiplication of integers induces a group structure on the set $(\mathbb{Z}/\langle m \rangle)^{\times}$.

ii. The ***totient*** $\phi(n)$ of a positive integer n is defined to be the number of positive integers less than or equal to n that are coprime to n. When $\gcd(r, m) = 1$, establish that $r^{\phi(m)} \equiv 1 \bmod m$.

iii. For any prime number p and any integer r, prove that $r^p \equiv r \bmod p$.

Solution.

i. Since multiplication of integers is associative and commutative with 1 as the identity, it induces an associative commutative binary operation on $\mathbb{Z}/\langle m \rangle$ with $\overline{1} := \langle m \rangle$ as an identity. When $\gcd(r, m) = 1$ and $\gcd(r', m) = 1$, there exists integers u, v, v', and v' such that $ru + mv = 1$ and $r'u' + mv' = 1$. Hence, we obtain $rr'(uu') + m(r'vu' + v') = r'(ru + mv)u' + mv' = r'u' + mv' = 1$, which implies that $\gcd(rr', m) = 1$. Thus, multiplication of integers induces an associative commutative binary operation on $(\mathbb{Z}/\langle m \rangle)^{\times}$ with $\overline{1}$ has an identity. Finally, the equation $ru + mv = 1$ implies that $\overline{r}\,\overline{u} = \overline{1}$ in $\mathbb{Z}/\langle m \rangle$, so each element of $(\mathbb{Z}/\langle m \rangle)^{\times}$ has an inverse. Therefore, the set $(\mathbb{Z}/\langle m \rangle)^{\times}$ is a group with respect to multiplication.

ii. From the definition of the totient function, we see that the order of the group $(\mathbb{Z}/\langle m \rangle)^{\times}$ is $\phi(m)$. From the Lagrange Theorem, we deduce that $\overline{r}^{\,\phi(m)} = \overline{1}$ for all $\overline{r} \in (\mathbb{Z}/\langle m \rangle)^{\times}$. In other words, we have $r^{\phi(m)} \equiv 1 \bmod m$.

iii. For any prime number p, we have $\phi(p) = p - 1$. When $r \equiv 0 \bmod p$, it follows that $r^p \equiv r \bmod p$. Otherwise, we have $r \not\equiv 0 \bmod p$ and $\gcd(r, p) = 1$ because p is prime. In this case, part *ii* yields $r^{p-1} \equiv 1 \bmod p$. Multiplying by r gives $r^p \equiv r \bmod p$. □

3. The ***icosahedral group*** I consists of the rotational symmetries of a regular dodecahedron. It acts transitively on the vertices, edges, and faces. Moreover, we have $|I| = 60$.

i. Determine the number of elements in I of each order.

ii. Determine the cardinality of each conjugacy class in I.

iii. Show that I is a simple group (i.e. it has no nontrivial normal subgroups).

Solution.

i. The icosahedral group I contains rotations by multiples of $2\pi/5$ about the centres of the faces, rotations by multiples of $2\pi/3$ about the vertices, and rotations by π about the centres of the edges. Each of the 20 vertices has a stabilizer of order 3. Since the opposite vertices have the same stabilizer, there are 10 subgroup of order 3. Each subgroup of order 3 contains two elements of order 3 and the intersection of any two of these subgroups consists of the identity, so I contains $(10)(2) = 20$ elements of order 3. Similarly, the faces have stabilizers of order 5, and there are six such stabilizers, giving $(6)(4) = 24$ elements of order 5. There are 15 stabilizers of edges and these stabilizers have order 2, so there are $(15)(1) = 15$ elements of order two. Finally the identity is the unique element of order 1. Since $60 = 1 + 15 + 20 + 24$, we have listed all the elements of the group.

ii. As conjugate elements have the same order, we consider four cases:

- The identity is the unique element in its conjugacy class.
- Since the edges form a single I-orbit, the stabilizers of the edges are conjugate subgroups. It follows that the nontrivial elements in these subgroups form one conjugacy class of cardinality 15.
- Consider a counterclockwise rotation x by $2\pi/3$ about a vertex v. Let v' be the opposite vertex and let x' be the counterclockwise rotation by $2\pi/3$ about v'. Since the vertices form a single I-orbit, their stabilizers are conjugate subgroups, so x and x' are conjugate. Moreover, the counterclockwise rotation x about v is the same as the clockwise rotation by $2\pi/3$ about the opposite vertex v'. Thus $x^2 = x'$, so x and x^2 are conjugate. Hence, all the elements of order 3 are conjugate.
- By considering the opposite face, a similar argument establishes that the 12 rotations by $2\pi/5$ and $-2\pi/5$ are conjugate. They are not conjugate to the remaining 12 rotations by $4\pi/5$ and $-4\pi/5$, because the order of a conjugacy class divides the order of the group and 24 does not divide 60. Thus, there are two conjugacy classes of elements of order 5.

Therefore, the class equation for I is $60 = 1 + 15 + 20 + 12 + 12$.

iii. Since a normal subgroup contains all the conjugates of its elements, a normal subgroup is a union of conjugacy classes. In particular, the order of a normal subgroup is the sum of some of the terms on the right side of the class equation including the term 1. It follows that a nontrivial normal subgroup of I must have order: 13, 16, 21, 25, 28, 33, 36, 40, 45, or 48. However, the Lagrange Theorem implies that the order of normal subgroup divides the order of the group. Therefore, the group I is simple. $\square$