
15.C.1. \( x^2 \in H \iff (xH)^2 = x^2 H = H \subseteq G/H \iff xH = (xH)^{-1} \subseteq G/H \). Thus \( x^2 \in H \) for every \( x \in G \) if and only if \( xH \) is its own inverse for every \( xH \subseteq G/H \).

15.C.2. \( x^m \in H \iff (xH)^m = x^m H = H \subseteq G/H \iff \text{ord}(xH)|m \). Thus \( x^m \in H \) for every \( x \in G \) if and only if the order of \( xH \) divides \( m \) for every \( xH \subseteq G/H \).

15.C.3. (Here the exercise is falsely stated; “an integer \( n \)” should be “a positive integer \( n \).” Here we prove the statement after this modification.)

If for every \( x \) there exists a positive integer \( n \) such that \( x^n \in H \), then \( x^n \in H \iff (xH)^n = x^n H = H \subseteq G/H \) thus \( \text{ord}(xH) \) is finite. Conversely, if every element of \( G/H \) has finite order then for any \( x \in G \) we have \( x^{\text{ord}(xH)} \in H \).


15.E.1. Since \( a^{\text{ord}(a)} = e \), \( (Ha)^{\text{ord}(a)} = He \). Thus \( \text{ord}(Ha)|\text{ord}(a) \).

15.E.2. This follows from Lagrange’s theorem and that \( |G/H| = (G : H) = m \).

15.E.3. By part 1 and 2, we have \( \text{ord}(Ha)|p \) and \( \text{ord}(Ha)|\text{ord}(a) \). Since \( a \notin H \), \( \text{ord}(Ha) \neq 1 \), thus \( \text{ord}(Ha) = p \) because \( p \) is a prime. Thus \( p|\text{ord}(a) \).


15.F.1. It follows from the assumption that \( \langle Ca \rangle = G/C \).

15.F.2. It directly follows from part 1.

15.F.3. Let us write \( x, y \in G \) to be \( x = ca^m, y = c'a^n \) for some \( c, c' \in C \). Then,

\[
xy = ca^m c'a^n = cc'a^{m+n} = c'a^n ca^m = yx.
\]

Thus \( xy = yx \).

15.F.4. It follows from part 3.

15.G.1. Let us write \([a]\) to be the conjugacy class of \(a\). Then,
\[
[a] = \{a\} \iff \{gag^{-1} \mid g \in G\} = \{a\} \iff gag^{-1} = a \ \forall g \in G \iff a \in C.
\]

15.G.2. After reordering \(k_1, k_2, \ldots, k_t\), we may assume that \(k_1, k_2, \ldots, k_{s-1}\) are the sizes of conjugacy classes in \(C\). By part 1, we have \(k_1 = k_2 = \cdots = k_{s-1}\) and also \(s - 1 = |C| = c\). Thus we have \(|G| = c + k_s + k_{s+1} + \cdots + k_t\) as desired.

15.G.3. We need to show that the size of \([x]\) is a power of \(p\) if \(x \notin C\). But we know that \(|[x]| = (G : C_x) = |G|/|C_x|\) where \(C_x\) is the centralizer of \(x\) in \(G\). In particular, \(|[x]| \mid |G| = p^k\). Thus \(|[x]|\) is a power of \(p\).

15.G.4. We know that \(k_i > 1\) for \(i \in \{s, s + 1, \ldots, t\}\) by part 1. Thus by part 3, \(k_i\) are multiple of \(p\). Now if we divide both sides of \(|G| = c + k_s + k_{s+1} + \cdots + k_t\) by \(p\), then we have \(c \equiv 0 \mod p\), from which the result follows.

References