SAMPLE FINAL  SAMPLE SOLUTIONS

1. By one of our subgroup criteria, it is enough to prove that \( x \cdot y^{-1} \in H \) whenever \( x, y \in H \). Obviously \( y^{-1} = 1/y \) in our group \( (\mathbb{R}^*, \cdot) \). So pick \( x, y \in H \) arbitrarily. Then \( x = a + b\sqrt{2} \) and \( y = c + d\sqrt{2} \) for some \( a, b, c, d \in H \). Then

\[
x \cdot y^{-1} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{(c + d\sqrt{2})(c - d\sqrt{2})} = \frac{ac - 2bd + bc\sqrt{2} - ad\sqrt{2}}{c^2 - 2d^2} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2}.
\]

So \( x \cdot y^{-1} \) is of the form \( a' + b'\sqrt{2} \) where

\[
a' = \frac{ac - 2bd}{c^2 - 2d^2} \quad \text{and} \quad b' = \frac{bc - ad}{c^2 - 2d^2}.
\]

Since \( a, b, c, d \in \mathbb{Q} \), we see that \( a', b' \in \mathbb{Q} \). Thus, \( x \cdot y^{-1} \in H \).

2. It is enough to verify that

(i) \( H \) is closed under \( \circ \);

(ii) The identity map \( \text{id} \) is in \( H \);

(iii) For each \( b \in H \) also the inverse map \( b^{-1} \in H \).

We check each item:

(i) Let \( b, c \in H \). We want to show that \( b \circ c \in H \). This amounts to showing that \( (b \circ c)[K] = K \). Now

\[
(b \circ c)[K] = b[c[K]] = b[K] = K.
\]

The second equality follows from the fact that \( c \in H \), i.e. \( c[K] = K \).

The last equality follows from the fact that \( b \in H \), i.e. \( b[K] = K \).

(ii) \( \text{id}[K] = \{\text{id}(x) \mid x \in K\} = \{x \mid x \in K\} = K \), so \( \text{id} \in H \).
(iii) Let \( b \in H \), i.e. \( b[K] = K \). We show that \( b^{-1} \in H \), i.e. that \( b^{-1}[K] = K \).

To see that \( K \subseteq b^{-1}[K] \): Pick any \( x \in K \); we show that \( x \in b^{-1}[K] \), i.e. \( x = b^{-1}(x') \) for some \( x' \in K \). But it is enough to set \( x' = b(x) \). Then \( x' \in K \) since \( b[K] = K \). And \( b^{-1}(x') = b^{-1}(b(x)) = x \).

To see that \( b^{-1}[K] \subseteq K \). Let \( x \in K \); we show that \( b^{-1}(x) \in K \). Since \( b[K] = K \), there is some \( \bar{x} \in K \) such that \( x = b(\bar{x}) \). Then \( b^{-1}(x) = b^{-1}(b(\bar{x})) = \bar{x} \in K \).

Another proof of (iii) suggested by your colleague during the last session:

\[
b^{-1}[K] = b^{-1}[b[K]] = (b^{-1} \circ b)[K] = K.
\]

The first equality follows from our assumption that \( K = b[K] \).

3. To see that \((G, \ast)\) is a group, we have to verify that \((G, \ast)\) is an associative structure, has the identity element and each \( f \in G \) has its inverse in \( G \).

(i) Associativity of \( \ast \): Choose any \( f, g, h \in G \). We show that \( f \ast (g \ast h) = (f \ast g) \ast h \). To see this, we show that \( (f \ast (g \ast h))(x) = ((f \ast g) \ast h)(x) \) for all \( x \in \mathbb{Z} \). Now

\[
\begin{align*}
(f \ast (g \ast h))(x) & = f(x) +_3 g \ast h(x) = f(x) +_3 (g(x) +_3 h(x)) \\
((f \ast g) \ast h)(x) & = (f \ast g)(x) +_3 h(x) = (f(x) +_3 g(x)) +_3 h(x) \\
& = f(x) +_3 (g(x) +_3 h(x)).
\end{align*}
\]

The last equality on the bottom line follows from the associativity of the operation \( +_3 \).

(ii) Identity element: Obviously, the map \( f_0 \) defined by \( f_0(x) = 0 \) is the identity element of \((G, \ast)\): If \( f \in G \) is arbitrary, we have

\[
(f \ast f_0)(x) = f(x) +_3 f_0(x) = f(x) +_3 0 = f(x),
\]

i.e. \( f \ast f_0 = f \). Similarly we show that \( f_0 \ast f = f \).

(iii) Inverse elements: Let \( f \in G \). We show that the function \( f' : \mathbb{Z} \to \mathbb{Z}_3 \) defined by

\[
f'(x) = \text{the inverse element to } f(x) \text{ in } (\mathbb{Z}_3, +_3)
\]
is the inverse to \( f \) in \((G, \ast)\). For this we need to show that \( f \ast f' = f_0 \) and \( f' \ast f = f_0 \). We prove just the former, the latter is proved similarly. Regarding the former, it is enough to prove that \( f \ast f'(x) = f_0(x) \) for all \( x \in \mathbb{Z} \). But

\[
f \ast f'(x) = f(x) + 3 \cdot f'(x) = 0 = f_0(x).
\]

4. Regarding (a). By our theory, a number \( a \in \mathbb{Z}_{24} \) is a generator of the group \((\mathbb{Z}_{24}, +_{24})\) just in case that \( \langle a \rangle = \mathbb{Z}_{24} \). This happens iff \( \langle a \rangle = \langle 1 \rangle \), which in turn is the case iff \( \gcd(a, 24) = 1 \). So the following numbers are generators of \((\mathbb{Z}_{24}, +_{24})\): 1, 5, 7, 11, 13, 17, 19.

Regarding (b): According to to our theory, the order of \( \langle a \rangle \) is equal to the order of \( \langle \gcd(a, 24) \rangle \), which is equal to 24/\( \gcd(a, 24) \). Thus, \( \langle a \rangle \) has 6 elements iff \( 24/\gcd(a, 24) = 6 \) iff \( \gcd(a, 24) = 4 \). So \( a \) is either 4 or 20.

5. Regarding (a). The permutation \( \sigma \) acts as follows: 1 \( \mapsto \) 5 \( \mapsto \) 9 \( \mapsto \) 6 \( \mapsto \) 1, 2 \( \mapsto \) 3 \( \mapsto \) 7 \( \mapsto \) 2 and 4 \( \mapsto \) 10 \( \mapsto \) 8 \( \mapsto \) 4. These are the disjoint cycles, i.e.

\[
\sigma = (1, 5, 9, 6)(2, 3, 7)(4, 10, 8).
\]

By our theory, the order of \( \sigma \) is the smallest common multiple of the lengths of these disjoint cycles, i.e. it is equal to the \( \text{scm}(4, 3, 3) = 12 \).

Regarding (b). We express each of the above cycles as a product of transpositions.

\[
(1, 5, 9, 6) = (1, 6)(1, 9)(1, 5) \\
(2, 3, 7) = (2, 7)(2, 3) \\
(4, 10, 8) = (4, 8)(4, 10)
\]

Thus,

\[
\sigma = (1, 6)(1, 9)(1, 5)(2, 7)(2, 3)(4, 8)(4, 10).
\]

So \( \sigma \) is a product of 7 transpositions, which means that the signum of \( \sigma \) is 1.

6. Regarding (a). Since \( h : \mathbb{Z} \rightarrow \mathbb{Z}_9 \) is a homomorphism, \( h(100) = h(1 \cdot 100) = (h(1))^{100} \) where the last power is computed in the group \((\mathbb{Z}_9, +_9)\). Thus, this power is equal to \( \text{rm}(h(1) \cdot 100, 9) = \text{rm}(5 \cdot 100, 9) = \text{rm}(500, 9) = 5 \).
Ker\((h)\) is a subgroup of \((\mathbb{Z}, +)\) and since \((\mathbb{Z}, +)\) is cyclic, so is Ker\((h)\). By our theory, Ker\((h)\) is not trivial, since \(h\) is not injective (there cannot be an injective map from an infinite set into a finite set). Again by our theory, the generator of Ker\((h)\) is the smallest positive number \(a\) such that \(a \in\) Ker\((h)\), i.e. such that \(h(a) = 0\). By the previous paragraph, \(h(a) = 5^a\) where the power on the right is computed in the group \((\mathbb{Z}_9, +)\). So we are looking for the least positive \(a\) such that \(5^a = 0\) in the group \((\mathbb{Z}_9, +)\). Such \(a\) is the order of \(5\) in \((\mathbb{Z}_9, +)\). By our theory, this order is equal to \(9 / \gcd(5, 9) = 9\). Thus, Ker\((h) = (9) = 9\mathbb{Z}\).

Regarding (b), the number \(5\) is a generator of the group \((\mathbb{Z}_{12}, +)\) since \(\gcd(5, 12) = 1\). Since \(9 = \text{rm}(5 \cdot 9, 12)\), in this group we have \(9 = 5^9\), so

\[
   h'\(9\) = (h'\(5\))^9 = \left((1, 4)(2, 3, 5)\right)^9 = (1, 4)^9(2, 3, 5)^9 = (1, 4).
\]

The third equality follows from the fact that disjoint cycles commute. Regarding the last equality: The order of \((2, 3, 5)\) is its length \(3\), so \((2, 3, 5)^9\) is the identity since \(3 \mid 9\). Similarly, the order of \((1, 4)\) is \(2\), so \((1, 4)^9 = (1, 4)^\text{rm}(9, 2) = (1, 4)^1 = (1, 4)\).

Similarly as in (a), Ker\((h')\) is a cyclic subgroup of \((\mathbb{Z}_{12}, +)\). Its generator has the form \(5^a\) where \(a\) is least possible, i.e. \(a\) is the least number in \(\mathbb{Z}_{12}\) such that \((h'(5))^a\) is the identity. So \(a\) is the order of \(h'(5) = (1, 4)(2, 3, 5)\). Now the order of this permutation is the smallest common multiple of their lengths, i.e. it is \(\text{scm}(2, 3) = 6\). Thus, Ker\((h') = \langle 5^6 \rangle\) where the power is computed in the group \((\mathbb{Z}_{12}, +)\). But \(5^6\) in this group is equal to \(\text{rm}(5 \cdot 6, 12) = 6\). Thus, Ker\((h') = \langle 6 \rangle\).

7. The index of \(\langle \sigma \rangle\) in \(S_6\) is equal to \(\text{order}(S_6) / \text{order}(\langle \sigma \rangle)\). Now:
   - \(\text{order}(S_6) = 6!\).

In order to determine the order of \(\sigma\), we have to express it as a product of disjoint cycles. The cycles in the assignment are not disjoint. So

\[
   \sigma = \left( \begin{array}{cccccc}
   1 & 2 & 3 & 4 & 5 & 6 \\
   5 & 1 & 2 & 6 & 4 & 3
   \end{array} \right)
\]

So the permutation \(\sigma\) is itself a cycle, namely

\[
   \sigma = (1, 5, 4, 6, 3, 2).
\]

Thus, the order of \(\sigma\) is its length, which is \(6\). Hence the index \(S_6 : \langle \sigma \rangle\) is equal to \(6! / 6 = 5! = 120\).