Problem Set #3

1 Modular arithmetic

Exercise 1:
Check that $\gcd(k, n) = 1$ and find $[k]^{-1}$ in $\mathbb{Z}/n\mathbb{Z}$ when $k = 296$, $n = 1317$.

Solution:

\[
gcd(296, 1317) = gcd(133, 296) = gcd(30, 133) = gcd(13, 30) = gcd(4, 13)
\]

\[
1317 = 4(296) + 133
\]

\[
296 = 2(133) + 30
\]

\[
133 = 4(30) + 13
\]

\[
30 = 2(13) + 4
\]

\[
13 = 4 \times 3 + 1
\]

So $gcd(296, 1317) = 1$, as claim. To find $r, s$ at $r(296) + s(131) = 1$ work the calculation backward

\[
1 = -3(4) + 1(13)
\]

\[
1 = -3(30 - 2(13)) + 1 \times 13 = 7 \times 13 - 3 \times 30
\]

\[
1 = 7(133 - 4(38) - 3(30) = -31(30) + 7(133)
\]

\[
1 = -31(296 - 2(133)) + 7(133) = 69(133) - 31(296)
\]

\[
1 = 69(1312 - 4(296)) - 31(296) = 69(1317) - 307(296)
\]

modulo $n = 1317$ we have $1 \equiv 0 - 307(296)$. We rewrite as $1 \equiv a \cdot 296 \ mod \ 1317$ with $0 \leq a < 1317$. Take $a = 1317 - 307 = 1010$; then $1010 \equiv -307 \ (mod \ n)$ and we get $[296]^{-1} = [1010]$ in $\mathbb{Z}/1317\mathbb{Z}$.

Exercise 2:
Determine $[a]^{-1}$ for each of the multiplicative units $[a] = [1], [5], [7], [11]$ in $\mathbb{Z}/12\mathbb{Z}$.

Solution:


These are so easy to compute we can use simple trial and errors or the extended euclidean algorithm to find that $[5]^{-1} = [5]$, since $5 \times 5 \equiv 25 \equiv 1 \ mod \ 12$. Similarly, $[7]^{-1} = [7]$,


1
Exercise 3:
Identify all element in \(\mathbb{Z}/18\mathbb{Z}\) that have multiplicative inverse. Find \([5]^{-1}\) in this system by finding \(r, s\) such that \(5r + 18s = 1\).

**Solution:**
\([k]\) has an inverse in \(\mathbb{Z}/18\mathbb{Z}\) \(\leftrightarrow k \neq 0\) and \(gcd(k, 18) = 1\). This "group of units" \(U_{18}\) is \(\{1, [5], [7], [11] = [−7], [13] = [−5], [17] = [−1]\}\). Although the extended GCD algorithm would provide suitable \(r, s\) we have for example \(-7(5) + 2(18) = 1\) (you can also use trial and error if you are lucky to find \(r, s\) quickly. Mod 18, \([-7][5] = [1]\) and \([5]^{-1} = [−7] = [11]\) (representative normalized to be in range \(0 \leq k \leq 18\).

2 Rationals

Exercise 4:
Prove that \(\sqrt{3}\) is irrational.

**Solution:**
If not \(\exists r, s \in \mathbb{Z}\), such that \(s \neq 0\) and \(r_3 = r/3\) and hence squaring both sides, \(3 = r^2/s^2\) or \(3s^2 = r^2\). We can assume that \(r\) and \(s\) have no prime divisor in common, otherwise, we may cancel them thus we assume \(gcd(r, s) = 1\). Now, \(3s^2 = r^2\). We can assume \(r\) and \(s\) have no prime divisors in common, otherwise we may cancel them; thus we assume \(gcd(r, s) = 1\). Now \(3s^2 = r^2 \Rightarrow 3|r^2\) but since 3 is a prime this implies \(3|r\), then \(3^2|r^2\), so that \(r^2 = m \cdot 3^2\) for some \(m \in \mathbb{Z}\). Thus, \(3s^2 = 3^2 \cdot m\). Canceling a "3" from each side we get \(s^2 = 3 \cdot m\) which implies \(3|s^2 \Rightarrow 3|5\). Thus 3 would divide both \(r\) and \(s\), contrary to our assumption that \(r, s\) have no prime divisor in common. Contradiction. Conclusion, \(\sqrt{3}\) cannot be rational.

3 Groups/Subgroups

Exercise 5:
Which of the following set are groups? (Explain your answer.)
1. \((\mathbb{Z}, \cdot)\);
2. \((\mathbb{R}, \cdot)\);
3. \(((\mathbb{Z}/7\mathbb{Z})^\times, \cdot)\);

**Solution:**
1. In \(S_3\), \((1, 2) \circ (1, 3)\) maps \(1 \to 3 \to 3, 2 \to 2 \to 1\) and \(3 \to 1 \to 2\). So the product is the 3-cycle (1, 3, 2).
2. \((1, 2) \circ (1, 3) = (1, 3, 2)(4)(5) = (1, 3, 2)\) in \(S_5\);
3. \((1, 5)(1, 4)(1, 3)(1, 2)\) maps \(1 \to 2 \to \cdots \to 2, 2 \to 1 \to 3 \to \cdots \to 3, \ldots\)
   \(5 \to 5 \ldots 5 \to 1\), so the product is \((1, 2, 3, 4, 5)\) is a 5-cycle.

Exercise 6:
Prove that
1. Knowing that \((\mathbb{Z}, +)\) is a group, prove that \((\mathbb{Z}/n\mathbb{Z}, \oplus)\) is a group;
2. Knowing that \((\mathbb{R}, +)\) is a group, prove that \((\mathbb{R}^n, +)\) is a group;

**Exercise 7:**

Prove that

1. Prove that \((\Omega_n, \cdot)\) is a subgroup of \((\mathbb{C}^\times, \cdot)\), where \(\Omega_n = \{z \in \mathbb{C} : z^n = 1\}\).
2. Prove that the orthogonal group \((O_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) : MM^T = I_n\}, \cdot)\) is a subgroup of \((GL_n(\mathbb{R}), \cdot)\).
3. Prove that the three-dimensional **Heisenberg group** of quantum mechanics consists of all real \(3 \times 3\) matrices of the form

\[
A = \begin{pmatrix}
1 & x & z \\
0 & 1 & y \\
0 & 0 & 1
\end{pmatrix}
\]

with \(x, y, z \in \mathbb{R}\) forms a subgroup of \((GL_n(\mathbb{R}), \cdot)\).
4. Prove that if \((G, \cdot)\) is a group and \(S \subset G\) non empty subset,
   (a) \(Z(G) = \{x \in G : gx = xg\ \text{for all} \ g \in G\}\) is a subgroup of \(G\);
   (b) \(Z_G(S) = \{x \in G : xs = sx\ \text{for all} \ s \in S\}\) is a subgroup of \(G\);
   (c) \(N_G(S) = \{x \in G : xSx^{-1} = S\}\) is a subgroup of \(G\).
   (d) If \(H_\alpha (\alpha \in I)\) are subgroups of \(G\), prove \(H = \cap_{\alpha \in I} H_\alpha\) is also a subgroup.
5. Suppose \(\phi : (G, \cdot) \rightarrow (G', \ast)\) is a homomorphism of groups, \((e \ \text{identity element of} \ \ G \text{and} \ e' \ \text{identity element of} \ G')\), prove that
   (a) \(\text{Ker}(\phi) = \{x \in G : \phi(x) = e'\}\) ,
      is a subgroup of \(G\)
   (b) \(\text{Range}(\phi) = \phi(G) = \{\phi(x) : x \in G\}\)
      is a subgroup of \(G'\).

**Exercise 8:**

Evaluate the net action of the following product of cycles:
1. \((1, 2)(1, 3)\) in \(S_3\);
2. \((1, 2)(1, 3)\) in \(S_5\);
3. \((1, 5)(1, 4)(1, 3)(1, 2)\) in \(S_5\);

**Solution:**

1. \((1, 2)^{-1} = (1, 2)\) since \((1, 2) \circ (1, 2) = Id\);
2. \((1, 2, 3)^{-1} = (1, 3, 2)\). Just check that \((1, 2, 3) \circ (1, 3, 2) = Id\);
3. \((i_1, i_2)^{-1} = (i_1, i_2)\); (The 2-cycle is its own inverse.)
4. $\sigma = (i_1, i_2, \ldots, i_k)$ then $\sigma^{-1} = (i_1, i_k, i_{k-1}, \ldots, i_2)$ (Just view as cyclic 1-step shifts in the diagram at right: $\sigma$ moves clockwise $\sigma^{-1}$ moves counter clockwise.

**Exercise 9:**
Find the inverses $\sigma^{-1}$ in $S_5$:

1. $(1, 2)$;
2. $(1, 2, 3)$;
3. For any cycle $(i_1, i_2)$ with $i_1 \neq i_2$;
4. $(i_1, i_2, \ldots, i_k)$ with $i_k \neq i_l$ for $k \neq l$.

**Solution:**

1. $(1, 2)^{-1} = (1, 2)$ since $(1, 2) \circ (1, 2) = Id$;
2. $(1, 2, 3)^{-1} = (1, 3, 2)$. Just check that $(1, 2, 3) \circ (1, 3, 2) = Id$;
3. $(i_1, i_2)^{-1} = (i_1, i_2)$; (The 2-cycle is its own inverse.)
4. $\sigma = (i_1, i_2, \ldots, i_k)$ then $\sigma^{-1} = (i_1, i_k, i_{k-1}, \ldots, i_2)$ (Just view as cyclic 1-step shifts in the diagram at right: $\sigma$ moves clockwise $\sigma^{-1}$ moves counter clockwise.)