Problem 1. Determine the order of

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

in $GL(4, \mathbb{R})$. What is $\langle A \rangle$ isomorphic to?

$$A^2 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, A^3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Therefore, $\text{ord}_{GL(4,\mathbb{R})}(\langle A \rangle) = 3$. Since $\text{ord}_{GL(4,\mathbb{R})}(\langle A \rangle) = 3$ and I know that $\text{ord}_{\langle \mathbb{Z}_3, + \rangle}(1) = 3$ I infer that $\langle A \rangle \cong \langle \mathbb{Z}_3, + \rangle$. This can be shown to be true.

Problem 2. Consider the following permutations in S_6:

$$\sigma_1 = (1), \quad \sigma_2 = (1,2)(3,6)(4,5), \quad \sigma_3 = (1,3)(2,5)(4,6), \quad \sigma_4 = (1,4)(2,6)(3,5),$$

$$\sigma_5 = (1,5,6)(2,3,4), \quad \sigma_6 = (1,6,5)(2,4,3)$$

Under the usual operations, it can be shown that they form a subgroup S.

(a) Complete the operation table for S.

(b) Is S abelian? Explain.

(c) Complete the operation table for D_3.

(d) Show that $S \cong D_3$ by rewriting the operation table of S to indicate the correspondence of the elements between the two groups.

(a)

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_6	σ_5	σ_4	σ_3
σ_3	σ_3	σ_5	σ_1	σ_6	σ_2	σ_4
σ_4	σ_4	σ_6	σ_5	σ_1	σ_3	σ_2
σ_5	σ_5	σ_3	σ_4	σ_2	σ_6	σ_1
σ_6	σ_6	σ_4	σ_2	σ_3	σ_1	σ_5

(b) No, because $\exists \sigma_i, \sigma_j \in S \; s.t \; \sigma_i \circ \sigma_j \neq \sigma_j \circ \sigma_i$

(c)

$\circ$	R_0	R_{120}	R_{240}	F_1	F_2	F_3
R_0	R_0	R_{120}	R_{240}	F_1	F_2	F_3
R_{120}	F_{120}	R_{240}	R_0	F_2	F_3	F_1
R_{240}	R_{240}	R_0	R_{120}	F_3	F_1	F_2
F_1	F_1	F_2	F_3	R_0	R_{120}	R_{240}
F_2	F_2	F_3	F_1	R_{240}	R_0	R_{120}
F_3	F_3	F_1	F_2	R_{120}	R_{240}	R_0

(d)

$\circ$	σ_1	σ_5	σ_6	σ_2	σ_3	σ_4
σ_1	σ_1	σ_5	σ_6	σ_2	σ_3	σ_4
σ_5	σ_5	σ_6	σ_1	σ_3	σ_4	σ_2
σ_6	σ_6	σ_1	σ_5	σ_4	σ_2	σ_3
σ_2	σ_2	σ_4	σ_3	σ_1	σ_6	σ_5
σ_3	σ_3	σ_2	σ_4	σ_5	σ_1	σ_6
σ_4	σ_4	σ_3	σ_2	σ_6	σ_5	σ_1

Problem 3. Let $H = \langle 2 \rangle \leq \mathbb{Z}_{12}$. Show that $H \cong U_6$.

To show that $H \cong U_6$ I will show that there is a well defined function $\phi : H \to U_6$ such that ϕ forms a bijection and is operation preserving. This function is defined as

$$\phi(x) = e^{\frac{x\pi i}{6}}, \ x \in H.$$

This is well defined because the computation is always possible (it is a substitution) and the images are within the codomain because everything in U_6 takes the form $e^{\frac{2\pi ki}{6}}$ and $\phi(x)$ raises e to some number in H, which are multiples of two, then multiplies that number in H by πi and divides by 6. So, clearly the elements in U_6 take the same form of the output of $\phi(x)$.

To show that there is a bijection I must show that ϕ is one-to-one and onto. Assume $\phi(x_1) = \phi(x_2)$, it follows that $e^{\frac{x_1\pi i}{6}} = e^{\frac{x_2\pi i}{6}}$. If I take the natural log of both sides I get, $\frac{x_1\pi i}{6} = \frac{x_2\pi i}{6}$. Dividing both sides by $\frac{\pi i}{6}$ I get $x_1 = x_2$. Since $\phi(x_1) = \phi(x_2) \implies x_1 = x_2$, this shows that ϕ is one-to-one.

Since all elements in U_6 take the form $e^{\frac{2k\pi i}{6}}$, $k \in \{1, 2, 3, 4, 5\}$ and all elements in H take the form $2z$, $z \in \{1, 2, 3, 4, 5\}$ it's clear by substitution of $2k = 2z = x$ to see that for every element in $y \in U_6$, there is some $x \in H$ such that $\phi(x) = y$. This shows that ϕ is onto.

ϕ is also operation preserving. That is, $\phi(x_1 + x_2) = \phi(x_1) \cdot \phi(x_2)$. To show this I rewrite the left hand side as

$$\phi(x_1 + x_2) = e^{\frac{(x_1+x_2)\pi i}{6}}.$$

Now, I rewrite

$$\phi(x_1) \cdot \phi(x_2) = e^{\frac{x_1\pi i}{6}} \cdot e^{\frac{x_2\pi i}{6}} = e^{\frac{\pi i(x_1+x_2)}{6}}$$

Substiuting these into $\phi(x_1 + x_2) = \phi(x_1) \cdot \phi(x_2)$, I get $e^{\frac{(x_1+x_2)\pi i}{6}} = e^{\frac{\pi i(x_1+x_2)}{6}}$ which is true. This shows that ϕ is operation preserving. Since ϕ is well defined, forms a bijection between H and U_6, and is operation preserving ϕ is an isomorphism. Since an isomorphism exists between H and U_6, $H \cong U_6$.

Problem 4. Find an explicit formula for $f(x)$, where $f : \mathbb{Z}_{30} \to \mathbb{Z}_{30}$ is a group isomorphism with the property that $f(7) = 11$.

$$f(x) = 23x \pmod{30}, \ x \in \mathbb{Z}_{30}$$

This function is an isomorphism because it is well defined, forms a bijection and is operation preserving. This is well defined because the output is computable because it is integer multiplication and this function will always be in Z_{30} because of the modulo operation. This function also forms a bijection. Assume $f(x_1) \equiv f(x_2)$. This implies $23x_1 \equiv 23x_2$. if I multiply by 23^{-1} on both sides, I get $x_1 \equiv x_2$. This shows that the function is one-to-one. The function is also onto because for every element in $y \in \mathbb{Z}_{30}, \exists x \in \mathbb{Z}_{30}$ such that $f(x) = y$. Since the function is one-to-one and onto, this is a bijection. This function is also operation preserving. $f(x_1 + x_2) = 23(x_1 + x_2)$ and $f(x_1) + f(x_2) = 23x_1 + 23x_2 = 23(x_1 + x_2)$. Since $f(x_1+x_2) = f(x_1)+f(x_2) = 23(x_1+x_2)$, this shows that f is operation preserving. Since this function is well defined, forms a bijection and is operation preserving, it is an isomorphism. Also, $f(7) = 23 \cdot 7 \equiv 11 \pmod{30}$

Problem 5. Show that $\mathbb{Z}_9^* \cong \mathbb{Z}_6$.

Problem 6. Show that $S_4 \ncong D_{12}$

The number of elements in S_4 that have order n should be the same in S_4 as in D_{12}. If I look at the elements of order 12, I see that in D_{12}, there are 13 elements. Those are all of the reflections plus the one rotation element R_{180}. Now, in S_4, there are only a few elements. Those are

$$(1,2),(1,3),(1,4),(2,3),(2,4),(3,4),(1,2)(3,4),(1,3)(2,4) \text{ and } (1,4)(2,3).$$

So, in S_4 there are 9 elements of order 2 and in D_{12} there are 13 elements of order 2. Since these are not the same, this shows that $S_4 \ncong D_{12}$.

Problem 7. Here is another way to show that $S_4 \ncong D_{12}$. In D_{12}, there is a transformation of order 12. Show that no such element exists in S_4.

In D_{12}, the element with order 12 is $R_{\frac{360}{12}} = R_{30}$. There is no such element in S_4 because the elements in S_4 can be written in terms of cycles of sum length 4. By theorem 6.3.1, the order of the product of disjoint cycles is the LCM of the lengths of the disjoint cycles. Since the longest cycle length is 4, the maximum order in S_4 is 4. So, no element of order 12 exists in S_4.

Problem 8. Define a binary operation $*$ on $S = \mathbb{R}^2 - \{(0,0)\}$ as

$$(a,b) * (c,d) = (ac - bd, ad + bc).$$

(a) Show that $\phi : \langle S, * \rangle \to \langle \mathbb{C}^*, \cdot \rangle$ defined by $\phi((a,b)) = a - bi$ is an isomorphism.

(b) What is the identity element in $\langle S, * \rangle$?

(c) Since $\langle \mathbb{C}^*, \cdot \rangle$ is a group, it follows that $\langle S, * \rangle$ is also a group. What is the inverse of (a,b) in S?

(a)

(b) (1,0) because $(a,b) * (c,d) = (a(1) - b(0), a(0) + b(1)) = (a,b)$. So (1,0) is the element such that when any other element is multiplied by it you get that same element.

(c)

Problem 9. Let $S = \mathbb{R} - \{-1\}$. We have seen that $\langle S, * \rangle$ is a group, where $*$ is defined as

$$a * b = a + b + ab.$$

Show that $\langle \mathbb{R}^*, \cdot \rangle \cong \langle S, * \rangle$ by proving that $\phi : \mathbb{R}^* \to S$ is defined by

$$\phi(x) = x - 1$$

is an isomorphism.

ϕ is a well defined function because $\phi(x) = -1$ when $x = 0$ but that is not in the domain. Additionally, subtraction is closed in $\mathbb{R}$, so for any x in the domain, there is an element in the codomain. ϕ is also one-to-one.
To show this, assume $\phi(x_1) = \phi(x_2)$ is true. Then $\phi(x_1) = \phi(x_2) \implies x_1 = x_2$. This is shown by rewriting the left hand side showing that it is equal to the right hand side. The left hand side is rewritten as

$\phi(x_1) = \phi(x_2) = x_1 - 1 = x_2 - 1$. Adding one on both sides I get, $x_1 = x_2$. This shows that ϕ is one-to-one. ϕ is onto because for every element in the codomain of ϕ covers all of $\mathbb{R} - \{-1\}$. So, for every element $y \in S$, there must be an element $x \in \mathbb{R}^*$ such that $\phi(x) = y$.
ϕ is operation preserving because $\phi(x_1 + x_2) = \phi(x_1) * \phi(x_2)$. I can show this by rewriting the left hand side the right hand side and showing that they are equal. The left hand side of the equation can be rewritten as $\phi(x_1 \cdot x_2) = (x_1 \cdot x_2) - 1$. The right hand side of the equation can be rewritten as $\phi(x_1) * \phi(x_2) = x_1 - 1 * x_2 - 1 = x_1 - 1 + x_2 - 1 + (x_1 - 1)(x_2 - 1) = x_1 + x_2 - 2 + x_1 \cdot x_2 - x_1 - x_2 + 1 = x_1 \cdot x_2 - 1$. Since $\phi(x_1 \cdot x_2) = (x_1 \cdot x_2) - 1 = x_1 \cdot x_2 - 1$, this shows that ϕ is onto.
Since ϕ is a well defined function and forms a bijection between $\langle R^*, \cdot$ and $\langle S, * \rangle$ and is operation preserving, ϕ is an isomorphism. Since there's an operation between these two groups, $\langle R^*, \cdot \rangle \cong \langle S, * \rangle$.

Problem 10. Show that given any isomorphism $\phi : G \to \overline{G}$, we always have $\phi(a^{-1}) = (\phi(a))^{-1}$ for any $a \in G$. Be sure to show your steps and reasoning clearly.

Since ϕ is an isomorphism it is operation preserving. This means that $\phi(x_1 \circ x_2) = \phi(x_1) * \phi(x_2)$. I can use this to represent $\phi(a^n) = \underbrace{\phi(a) * \phi(a) * \cdots * \phi(a)}_{n} = [\phi(a)]^n$ when n is positive. When n is negative, $-n$ is positive and the positive case was just shown so, $\phi(a^{-n}) = [\phi(a)]^{-n}$. When $n = -1$, $\phi(a^{-1}) = (\phi(a^{-1}))$ is true.

Problem 11. Let $\phi : G \to \overline{G}$ be an isomorphism. Prove that if G is cyclic, then $\overline{G}$ is also cyclic.

Proof. Using theorem 7.4.1, and the proof of property 2 and 1, assume G is cyclic, since G is cyclic there is some $a \in G$ that generates G. Let n be the integer where $a^n = e$. Then, by property 1, $\phi(e) = \overline{e}$, and since $\phi(a^n) = \phi(e) = \overline{e}$, using property 2 and 1, it must be true that, $\phi(a^n) = [\phi(a)]^n = \overline{e}$. Since there is an n such that $[\phi(a)]^n = \overline{e}$, by definition of a cyclic group, $\overline{G}$ must be cyclic if G is cyclic. □

Problem 12. Let $\phi : G \to \overline{G}$ be a group isomorphism. Prove that if $\overline{H} \leq \overline{G}$, then $\phi^{-1}(\overline{H}) \leq G$.

Proof. By theorem 7.4.2, if $\phi : G \to \overline{G}$ is a group isomorphism, then ϕ^{-1} is also an isomorphism. Theorem 7.4.2 also states that if $H \leq G$, then $\phi(H) \leq \overline{G}$. Since $\phi^{-1} : \overline{G} \to G$ is an isomorphism and $\overline{H} \leq \overline{G}$, by theorem 7.4.2, $\phi^{-1}(\overline{H}) \leq G$. □

Problem 13. Let $\phi : G \to \overline{G}$ be a group isomorphism. Prove that $\phi^{-1} : \overline{G} \to G$ is also a group isomorphism.

Proof. Since ϕ is a bijection, by well known properties of bijections, ϕ^{-1} exists. ϕ^{-1} is also operation preserving because $\phi(x_1 \circ x_2) = x_3 \cdot x_4 \implies \phi^{-1}(x_3 \cdot x_4) = x_1 \circ x_2 = \phi(x_3)^{-1} \circ \phi(x_4)^{-1}$. Since $\phi^{-1} : \overline{G} \to G$, is a bijective function that is operation preserving it is an isomorphism. □

Problem 14. What are the automorphisms of $\mathbb{Z}_8$? Be sure to describe them clearly.

An automorphism of $\mathbb{Z}_8$ map 1 to another generator of $\mathbb{Z}_8$. So, a generator of $\mathbb{Z}_8$ is a coprime of 8. Those are 1,3,5,7. So if I define f_i such that $f_i(1) = i$, through a table it is easy to see that $\text{Aut}(\mathbb{Z}_8) = \{f_1, f_3, f_5, f_7\}$.