Math 71: Abstract Algebra

Prishita Dharampal

Bibliography: Talked to Sair Shaikh '26, Henry Dorr '28, Kason Sabazan-Chambers '28, and Math Stack Exchange.

Problem 1. Klein four. Define the Klein four group to the group with presentation

$$V_4 = \langle a, b \,|\, a^2 = b^2 = e, ab = ba \rangle$$

1. Prove that V_4 has 4 elements, and that each nonidentity element has order 2.
2. Prove that V_4 is isomorphic to $(\mathbb{Z}/8\mathbb{Z})^\times$ as well as isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.
3. Find every subgroup of S_4 isomorphic to V_4, and determine which are normal subgroups.

Solution.

1. From the presentation, V_4 can be generated by a, b and the maximum power they can have is 2 before they stop producing distinct elements. So, possible elements of V_4 are:

   (a) $a^0 = b^0 = e$

   (b) $a^1 = a$

   (c) $b^1 = b$

   (d) $a^2 = b^2 = (ab)^2 = a^2 \cdot b^2 = e$

   (e) $a^1 b^1 = ab$

   Hence, V_4 has 4 distinct elements. From (c) we can also see that all nonidentity elements have order 2.

2. (a) $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$
   Define a function $\varphi : V_4 \to (\mathbb{Z}/8\mathbb{Z})^\times$ such that:

   i. $\varphi(e) = 1$

ii. $\varphi(a) = 3$
iii. $\varphi(b) = 5$
iv. $\varphi(ab) = 15(\text{mod } 8) = 7(\text{mod } 8)$

And the orders of the elements are:

i. $\mid 1 \mid = 1$
ii. $3^2 = 9(\text{mod } 8) = 1(\text{mod } 8) \implies \mid 3 \mid = 2$
iii. $5^2 = 25(\text{mod } 8) = 1(\text{mod } 8) \implies \mid 5 \mid = 2$
iv. $7^2 = 49(\text{mod } 8) = 1(\text{mod } 8) \implies \mid 7 \mid = 2$

So, given the information above, we can write a presentation of $(\mathbb{Z}/8\mathbb{Z})^\times$:

$$(\mathbb{Z}/8\mathbb{Z})^\times = \langle 3, 5 \mid 3^2 = 5^2 = e, 3 \cdot 5 = 5 \cdot 3 \rangle$$

Which is similar to the presentation of V_4:

$$V_4 = \langle a, b \,| a^2 = b^2 = e, ab = ba \rangle$$

Thus the two groups are isomorphic.

(b) $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0)(1,1)\}$ Define a function $\varphi : V_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ such that:

i. $\varphi(e) = (0,0)$
ii. $\varphi(a) = (0,1)$
iii. $\varphi(b) = (1,0)$
iv. $\varphi(ab) = (1,1)$ Also, $\varphi(a) + \varphi(b) = (0,1) + (1,0) = (1,1) = \varphi(ab)$

And the orders of the elements are:

i. $\mid (0,0) \mid = 1$
ii. $(0,1)^2 = (0,1) + (0,1)(\text{mod } 2) = (0,2)(\text{mod } 2) = (0,0)(\text{mod } 2)$
$\implies \mid (0,1) \mid = 2$
iii. $(1,0)^2 = (1,0) + (1,0)(\text{mod } 2) = (2,0)(\text{mod } 2) = (0,0)(\text{mod } 2)$
$\implies \mid (1,0) \mid = 2$
iv. $(1,1)^2 = (1,1) + (1,1)(\text{mod } 2) = (2,2)(\text{mod } 2) = (0,0)(\text{mod } 2)$
$\implies \mid (1,1) \mid = 2$

So, given the information above, we can write a presentation of $\mathbb{Z}_2 \times \mathbb{Z}_2$:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle (0,1), (1,0) \mid (0,1)^2 = (1,0)^2 = e, (0,1) + (1,0) = (1,0) + (0,1) \rangle$$

Which is similar to the presentation of V_4:

$$V_4 = \langle a, b \,| a^2 = b^2 = e, ab = ba \rangle$$

Thus the two groups are isomorphic.

(c) For $\sigma \in S_4$ to be a part of a subgroup isomorphic to V_4, $\mid \sigma_a \mid = \mid \sigma_b \mid = \mid \sigma_a \sigma_b \mid = 2$. So that restricts us to 2 cycles and products of disjoint 2 cycles in S_4. If a, b were both products of disjoint 2-cycles, ab could be:

i. $a = (wx)(yz), b = (wx) \implies ab = (yz)$

ii. $a = (wx), b = (yz) \implies ab = (wx)(yz)$

iii. $a = (wx)(yz), b = (xy) \implies ab = (wx)(yz)(xy) = (ywxz)$
This cannot be the case because then ab has order 4.

iv. $a = (wx)(yz), b = (xy)(wz) \implies ab = (wx)(yz)(xy)(wz) = (xz)(wy)$

v. $a = (wx)(yz), b = (yz)(wx)$ but because disjoint cycles commute $a = b$, which is a contradiction.

vi. Other possible cases include $a = (wx)(yz), b = (wx)(wx)$ but then $\mid b \mid = 1$ which is a contradiction.

Of the above only (i), (ii), and (iv) are valid possibilities. And everything is it's own inverse (all non identity elements have order 2). So, the generic subgroups A of S_4 that are isomorphic to V_4 are of one of the two forms:

$$A = \{e, (wx), (yz), (wx)(yz)\}$$

or

$$A = \{e, (wx)(yz), (xy)(wz), (xz)(wy)\}$$

where w, x, y, z can be distinct elements from $\{1, 2, 3, 4\}$.
For A to be a normal subgroup of S_4, $sAs^{-1} \in A, \forall s \in S_4$.

Conjugation of a cycle:
Let $\sigma \in A$, $s \in S_4$.

$$\pi = s\sigma s^{-1}$$

Let $\sigma(i) = j$, $i \in \sigma$.

$$s\sigma(i)s^{-1}s = s\sigma(i) = s(j)$$
$$\pi(s(i)) = s(j)$$

Hence conjugating a permutation can only change the position of the elements in the permutation, not the cycle structure.

i. For $A = \{e, (wx), (yz), (wx)(yz)\}$ let's consider $(yw)(wx)(yw)$, (yw) has order 2 and is its own inverse.

$$(yw)(wx)(yw) = (w)(yx) = (yx)$$

$(yx) \notin A$, so all subgroup of this form are not normal.

ii. For $A = \{e, (wx)(yz), (xy)(wz), (xz)(wy)\}$: Conjugation of a cycle does not change the type of that cycle: so all 2 disjoint 2 cycles map to some other pair of 2 disjoint 2 cycles. But A has all possible two cycles. So $sAs^{-1} \in A$. Hence all subgroups A are normal subgroups of G.

Problem 2. Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps $\pi_1 : G \to A$ and $\pi_2 : G \to B$ defined by $\pi_1((a, b)) = a$ and $\pi_2((a, b)) = b$ are homomorphisms and find their kernels (cf. Exercise 14).

Solution.

For π_1 to be a homomorphism, the following has to be true for any $(a, b), (c, d) \in G$:

$$\pi_1((a, b) \cdot (c, d)) = \pi_1((a, b)) \cdot \pi_1((c, d))$$

so,

$$\pi_1((a, b) \cdot (c, d)) = \pi_1((a \cdot c, b \cdot d)) = a \cdot c = \pi_1((a, b)) \cdot \pi_1((c, d))$$

Hence, π_1 is a homomorphism. Also,

$$ker\, \pi_1 = \{\, (e_A, b) \in G \mid b \in B \,\}$$

Similarly, for π_2 we need to show that

$$\pi_2((a, b) \cdot (c, d)) = \pi_2((a, b)) \cdot \pi_2((c, d))$$

is true $\forall (a, b), (c, d) \in G$.

$$\pi_2((a, b) \cdot (c, d)) = \pi_2((a \cdot c, b \cdot d)) = b \cdot d = \pi_2((a, b)) \cdot \pi_2((c, d))$$

Hence, π_2 is a homomorphism. And,

$$ker\, \pi_2 = \{\, (a, e_B) \in G \mid a \in A \,\}.$$

Problem 3. Let G be a group and let $Aut(G)$ be the set of all isomorphisms from G onto G. Prove that $Aut(G)$ is a group under function composition (called the automorphism group of G and the elements of $Aut(G)$ are called automorphisms of G).

Solution.

To show that $Aut(G)$ is a group under $\circ$, where $f \circ g(x) = f(g(x))$, we need to show the following:

1. Closure under inverses:
   An isomorphism is a bijective homomorphism. Then, by definition if $g : G \to G$, $g \in Aut(G)$ is an isomorphism, there exists its inverse $g^{-1} : G \to G$ which is also an isomorphism. But because $Aut(G)$ is the set of all isomorphisms from $G \to G$, $g^{-1} \in Aut(G)$. Thus, $Aut(G)$ is closed under inverses.

2. Closure under function composition:

3. Identity:
   Let $i : G \to G$ be the identity map such that $i(a) = a, \forall a \in G$.
   $i(ab) = ab = i(a)i(b)$ so i is also an homomorphism. And i is obviously bijective $(a \to a, \forall a \in G)$, so i is an isomorphism in $Aut(G)$.

4. Associativity:
   For any $f, g, h \in Aut(G), x \in G$ we have to show that $f \circ (g \circ h(x) = (f \circ g) \circ h(x)$.

   $$f \circ (g \circ h(x)) = f \circ (g(h(x)) = f(g(h(x))),$$

   and

   $$(f \circ g) \circ h(x)) = (f \circ g)(h(x)) = f(g(h(x))),$$

   Thus, $Aut(G)$ is associative.

Problem 4. Assume n is an even positive integer and show that D_{2n} acts on the set consisting of pairs of opposite vertices of a regular n-gon. Find the kernel of this action (label vertices as usual).

Solution.

$$D_{2n} = \langle s, r \mid s^2 = r^n = 1, rs = sr^{-1} \rangle$$

Because D_{2n} is generated by r, s, to show that D_{2n} is a group action on the set containing pairs of opposite vertices of a regular n-gon, we only need to show that s and r are valid actions on the set.
$s, r \in D_{2n}$ can be arithmetically defined as :

$$s = n - m$$

$$r = m + 1$$

where n is the total number of vertices of the n-gon, and m is the vertex the operation is being performed on. Let A be the set of pairs of opposite vertices of a regular n-gon. To show that $D_{2n} \times A \to A$, the following must be true:

$$g_1 \cdot (g_2(x)) = (g_1 \cdot g_2)(x) \qquad \forall x \in S,\, g_1 g_2 \in D_{2n}$$

Inputting specifics,

$$\begin{aligned} s(r(a)) &= (sr)(a) \qquad \forall a \in A \\ (n-m)((m+1(a)) &= ((n-m)(m+1)(a) \end{aligned}$$

because m is the vertex the operation is currently being performed on and function composition moves from right to left, the eq above can be simplified as:

$$\begin{aligned} (n-m)((a+1)) &= ((n-(m+1)(a) \\ (n-(a+1)) &= n-(a+1) \\ n-a-1 &= n-a-1 \end{aligned}$$

But elements in A are pairs:

$$\begin{aligned} s(r((a,b))) &= (sr)((a,b)) \qquad \forall (a,b) \in A \\ (n-m)((m+1((a,b))) &= ((n-m)(m+1)(a,b) \\ (n-m)((a+1),(b+1)) &= ((n-(m+1)(a,b) \\ ((n-(a+1)),(n-(b+1)) &= (n-((a+1,b+1))) \\ ((n-a-1),(n-b-1)) &= ((n-a-1),(n-b-1)) \end{aligned}$$

Thus, D_{2n} acts on the Set A.
Right now, the only actions that send the vertices to their original positions are r^n and s^2. But because the ordering of the pairs doesn't really matter because the polygon is in the same physical place, any operation which sends all vertices to their opposites also gives the identity of the group; the only action that does this is $r^{n/2}$. It is also important to note that s is still not an identity because except for the vertices on the axis of symmetry every other pair exchanges vertices. For example, in D_{2n}, $s(2,5) = (6,3)$ when the line of symmetry is $(1,4)$. So the kernel of $D_{2n} = \{s^2, r^n, r^{n/2}\} = \{e, r^{n/2}\}$.

Problem 5. Show that the group of rigid motions of a tetrahedron is isomorphic to a subgroup (cf. Exercise 26 of Section 1) of S_4.

Solution.

If we label the vertices of the tetrahedron $\{1, 2, 3, 4\}$, then we can see that all rigid motions of a tetrahedron can be mapped to a permutation in S_4. Let's call the group of distinct rigid motions of a tetrahedron T, then this map can be defined as $\phi : T \to S_4$. For any $t, u \in T$ that map to permutations $\sigma_t, \sigma_u \in S_4$, we can see that $\phi(tu) = \sigma_t\sigma_u = \phi(t)\phi(u)$. Hence, ϕ is a homomorphism.
$\phi(t) = \phi(u) \implies t = u$, because if two rigid motions map to the same σ then they are not distinct. So ϕ is an injective homomorphism.
If we restrict the co-domain of ϕ to the image of ϕ then we have an isomorphism to a subset of S_4. To see if this subset is a subgroup we check for closure under the group operation and inverses:

1. Closure under inverses:
   $\forall t \in T, \exists\, t^{-1} \in T \implies \phi(t^{-1}) = \phi(t)^{-1} = \sigma_t^{-1}$. Hence ϕ is closed under inverses.

2. Closure under group action:
   From definition of the homomorphism defined, we see that for any $t, u \in T$,
   $\phi(t)\phi(u) = \sigma_t\sigma_u = \phi(tu)$. Hence ϕ is closed under inverses.

3. Because ϕ is closed under both, inverses and the group action $\exists\, e \in$ the subset, and thus, the subset is a subgroup of S_4.

Finally, we can say that the group of rigid motions T of a tetrahedron is isomorphic to a subgroup of S_4.

Problem 6. Let $G = GL_n(\mathbb{F})$, where $\mathbb{F}$ is any field. Define

$$SL_n(\mathbb{F}) = \{A \in GL_n(\mathbb{F}) \mid det(A) = 1\}$$

(called the special linear group.) Prove that $SL_n(\mathbb{F}) \leq GL_n(\mathbb{F})$.

Solution.

$$SL_n(\mathbb{F}) = \{A \in GL_n(\mathbb{F}) \mid det(A) = 1\}$$

To see if $SL_n(\mathbb{F})$ is a sub-group:

1. $det(I_n)$, where I_n is the identity matrix of order n, always has determinent 1, so $Sl_n(\mathbb{F})$ is non-empty and the identity exists in the sub-group.

2. Closure under inverses:
We know that for any matrices A, B, $det(AB) = det(A)det(B)$. So, when $AB = I_n$, and A is any $A \in SL_n(\mathbb{F})$:

$$\begin{aligned} det(A)det(A^{-1}) &= det(I_n) \\ 1.det(A^{-1}) &= 1 \\ det(A^{-1}) &= 1 \end{aligned}$$

So, $A^{-1} \in SL_n(\mathbb{F})$. Hence, $SL_n(\mathbb{F})$ is closed under inverses.

3. Closure under multiplication:
Similar to above, for any matrices $A, B \in SL_n(\mathbb{F})$:

$$\begin{aligned} det(A)det(B) &= det(AB) \\ 1.1 &= det(AB) \\ det(AB) &= 1 \end{aligned}$$

Hence, $AB \in SL_n(\mathbb{F})$.

Thus, $SL_n(\mathbb{F})$ is a subgroup.

Problem 7. Define $\varphi : \mathbb{R}^\times \to \{\pm 1\}$ by letting $\varphi(x)$ be x divided by the absolute value of x. Describe the fibers of φ and prove that φ is a homomorphism.

Solution.

$$\varphi : \mathbb{R}^\times \to \{\pm 1\}$$
$$\varphi(x) = \frac{x}{abs(x)} = \begin{cases} 1 & x > 0 \\ -1 & x < 0 \end{cases}$$

All positive numbers in $\mathbb{R}$ map to $+1$ because a positive number divided by it's own absolute value gives $+1$, and all negative numbers $\in \mathbb{R}$ map to -1 because $\frac{-x}{x} = -1$. So the fibers of φ are $\mathbb{R}^+$ and $\mathbb{R}^-$.

For φ to be a homomorphism, the following has to be true:

$$\varphi(ab) = \varphi(a)\varphi(b) \qquad \forall a, b \in \mathbb{R}^\times$$

We have four cases to check:

1. $a, b > 0$:
   $a, b > 0 \implies ab > 0$
   $\varphi(ab) = \frac{ab}{abs(ab)} = 1 = 1 \cdot 1 = \frac{a}{abs(a)} \cdot \frac{b}{abs(b)} = \varphi(a) \cdot \varphi(b)$

2. $a > 0,\ b < 0$:
   $a > 0,\ b < 0 \implies ab < 0$
   $\varphi(ab) = \frac{ab}{abs(ab)} = \frac{ab}{-ab} = -1 = 1 \cdot -1 = \frac{a}{a} \cdot \frac{b}{-b} = \frac{a}{abs(a)} \cdot \frac{b}{abs(b)} = \varphi(a) \cdot \varphi(b)$

3. $a < 0,\ b > 0$:
   Since a, b are arbitrary elements of $\mathbb{R}^\times$ and $\mathbb{R}^\times$ is abelian this case is the same as the one above.

4. $a, b < 0$:
   $a, b < 0 \implies ab > 0$
   $\varphi(ab) = \frac{ab}{abs(ab)} = 1 = -1 \cdot -1 = \frac{a}{-a} \cdot \frac{b}{-b} = \frac{a}{abs(a)} \cdot \frac{b}{abs(b)} = \varphi(a) \cdot \varphi(b)$

Thus, φ is a homomorphism.

Problem 8. Define $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x + y$. Prove that π is a surjective homomorphism and describe the kernel and fibers of π geometrically.

Solution.

For any $(a, b), (c, d) \in \mathbb{R}^2$,

$$\pi((a, b)+(c, d)) = \pi((a+c, b+d)) = (a+c)+(b+d) = (a+b)+(c+d) = \pi((a, b))+\pi((c, d))$$

so, π is a homomorphism. We can see that it is surjective because for any $a \in \mathbb{R}$, $\pi(a, 0) = a$. The kernel for this map is everything that maps to 0. $ker\, \pi = \{(a, -a) \mid \forall a \in \mathbb{R}\}$. The kernel of this map is a line that passes through origin with slope $= -1 = (-a/a)$. All other fibers of π are lines that pass through $(a, 0)$ for any $a \in \mathbb{R}$ with slope $= -1$. Hence, they are translations of the kernel over the x-axis.

Problem 9. Consider the additive quotient group $\mathbb{Q}/\mathbb{Z}$.

1. Show that every coset of $\mathbb{Z}$ in $\mathbb{Q}$ contains exactly one representative $q \in \mathbb{Q}$ in the range $0 \leq q < 1$.
2. Show that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order but that there are elements of arbitrarily large order.
3. Show that $\mathbb{Q}/\mathbb{Z}$ is the torsion subgroup of $\mathbb{R}/\mathbb{Z}$ (cf. Exercise 6, Section 2.1).
4. Prove that $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the multiplicative group of root of unity in $\mathbb{C}^\times$.

Solution.

1. If we define a homomorphism $\phi : \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$, we can see that the $ker\,\phi = \{\frac{p}{q} \in \mathbb{Q}; q \mid p\} = \{\mathbb{Z}\}$. So, $\forall z \in \mathbb{Q}$ where z is an integer maps to the identity. The cosets then can be defined as $q + \mathbb{Z}, q \in \mathbb{Q}$. Then, for any $z \in q + \mathbb{Z}$, we can write z as $n + r, n \in \mathbb{Z}, 0 \leq r < 1$.
   But because $\mathbb{Z}$ is in the kernel of ϕ,
   $$z = n + r$$
   $$z \equiv 0 + r$$
   $$z \equiv r$$
   So, $\forall z$ there exists a representative in $0 \leq r < 1$. Assume that representative of z is not unique, then:
   $$\mathbb{Z} + r_1 = \mathbb{Z} + r2$$
   $$r_1 - r_2 \in \mathbb{Z}$$
   by group operation on cosets. We know that in $0 \leq r_1, r_2 < 1$, the only integer is:
   $$r_1 - r_2 = 0$$
   $$r_1 = r_2$$
   Which is a contradiction. Thus, the presentation of all cosets have exactly one representative in the range $[0, 1)$.

2. All elements in $\mathbb{Q}/\mathbb{Z}$ can be representative as p/q, $gcd(p, q) = 1, p < q$. To find the order of this element we need to add p/q to itself enough times to give an integer, i.e.
   $$\frac{p}{q} \cdot n = p \implies n = q$$

the order of an element in $\mathbb{Q}/\mathbb{Z}$ is equal to it's denominator, when represented like described above. However, q can be an arbitrarily large number which is why the order can be arbitrarily large. When $q = \infty \implies 1/q = 0 \implies \mid 0 \mid = 1$. Hence, we cannot have infinite order.

3. A torsion subgroup is a an abelian subgroup in which all elements have finite order. Things we know about $\mathbb{Q}/\mathbb{Z}, \mathbb{R}/\mathbb{Z}$:

   (a) $\mathbb{Q}/\mathbb{Z}$ is a subgroup of $\mathbb{Q}$, and inherits the abelian properties.

   (b) $\mathbb{Q} \subseteq \mathbb{R} \implies \mathbb{Q}/\mathbb{Z} \subseteq \mathbb{R}/\mathbb{Z}$

   (c) from (2), we know that $\forall \frac{p}{q} \in \mathbb{Q}/\mathbb{Z}, \mid \frac{p}{q} \mid < \infty$.

   Thus because $\mathbb{Q}/\mathbb{Z}$ is a subgroup of $\mathbb{R}/\mathbb{Z}$, and all elements have finite order $\mathbb{Q}/\mathbb{Z}$ is a torsion subgroup of $\mathbb{R}/\mathbb{Z}$.

4. Multiplicative groups of roots of unity contain: $e^{2\pi i \frac{k}{n}}$, where n is the n-th root of unity, and $0 \leq k < n - 1$. All elements in $\mathbb{Q}/\mathbb{Z}$ can be represented as $\frac{k}{n}$, in their lowest forms. Define $\phi : \mathbb{Q}/\mathbb{Z} \to$ multiplicative group of roots of unity in $\mathbb{C}^{\times}$, $\phi(\frac{k}{n}) = e^{2\pi i \frac{k}{n}}$.
   Now, to check if ϕ is an isomorphism:

   (a) Check if ϕ is injective:
   Let $e^{2\pi i \frac{a_1}{b_1}} = e^{2\pi i \frac{a_2}{b_2}}$,

   $$\begin{aligned} e^{2\pi i \frac{a_1}{b_1}} &= e^{2\pi i \frac{a_2}{b_2}} \\ ln(e^{2\pi i \frac{a_1}{b_1}}) &= ln(e^{2\pi i \frac{a_2}{b_2}}) \\ 2\pi i \frac{a_1}{b_1} &= 2\pi i \frac{a_2}{b_2} \\ \frac{a_1}{b_1} &= \frac{a_2}{b_2} \end{aligned}$$

   If $\phi(a) = \phi(b) \implies a = b$, then ϕ is injective.

   (b) Check if ϕ is surjective:
   By definition $\phi : \frac{k}{n} \to e^{2\pi i \frac{k}{n}}, \forall \frac{k}{n} \in \mathbb{Q}/\mathbb{Z}$. Hence ϕ is surjective.

   Hence, ϕ is a bijective homomorphism or an isomorphism.

Problem 10. Fields of order 4.

1. Let $F = \{0, 1, x, y\}$. Prove that there are operations $+$ and $\cdot$ on F, such that $1 + x = y$ and $x^2 = y$, making F into a field. (Note that the four elements of F are distinct!) Essentially the problem is to fill out the addition and multiplication tables: You already know certain rows and columns by properties of 0 and 1 in a field!

+	0	1	x	y
0				
1				
x				
y				

.	0	1	x	y
0				
1				
x				
y				

2. Let F_1 and F_2 be fields. A map $\phi : F_1 \to F_2$ is an isomorphism of fields if ϕ is a bijection satisfying $\phi(x + y) = \phi(x) + \phi(y)$ and $\phi(xy) = \phi(x)\phi(y)$ and $\phi(1_{F_1}) = 1_{F_2}$. An isomorphism between a field and itself is called an automorphism. Find a non-identity automorphism of the field F of order 4 described above.

3. Let F' be any field with 4 elements. Prove that there exists an isomorphism $\phi : F \to F'$, where F is the field described above.

This shows that there is a unique "isomorphism class" of field of order 4, which we call $\mathbb{F}_4$.

Solution.

1. Just from the given properties we can fill out the tables like so:

+	0	1	x	y
0	0	1	x	y
1	1		y	
x	x	y		
y	y			

.	0	1	x	y
0	0	0	0	0
1	0	1	x	y
x	0	x	y	
y	0	y		

To determine the other elements:

(a) For multiplication: The multiplicative group is $= \{1, x, y\}$. So the max order an element in this group can have is 3. Non-identity element can only have orders $\{2, 3\}$.
$xy = x \cdot x^2 = x^3$
If $\mid x \mid = 2 : x^2 = 1 \implies y = 1$ But $y, 1$ are distinct elements (by definition), so $\mid x \mid \neq 2$. So $x^3 = 1$. Then, $y^2 = x^4$ but $x^3 = 1$ so, $y^2 = x^3 \cdot x = x$.

.	0	1	x	y
0	0	0	0	0
1	0	1	x	y
x	0	x	y	1
y	0	y	1	x

(b) For addition: The additive group is = $\{0, 1, x, y\}$, and because order of the element has to divide order of the group the possible orders are only $\{1, 2, 4\}$. Again, all non-identity elements have order $\neq 1$. So, $1, x, y$ have orders equal to either 2 or 4. Assume $\mid 1 \mid = 4$, let $x = 1 + 1$,

$$x = 1 + 1 = xx^{-1} + xx^{-1} = x^{-1}(x + x) = x^{-1}(2x) = x^{-1}(0) = 0.$$

But this is a contradiction to the function definition, because $x, 0$ are distinct elements. So the order of 1 has to be 2.
Next,

$$x + x = x(1 + 1) = x(0) = 0$$
$$y + y = y(1 + 1) = y(0) = 0$$

So both x, y have order 2.
Next,

$$y + 1 = x + 1 + 1 = x + 0 = x$$
$$y + x = x + 1 + x = 2x + 1 = 0 + 1 = 1$$

+	0	1	x	y
0	0	1	x	y
1	1	0	y	x
x	x	y	0	1
y	y	x	1	0

Finally,

.	0	1	x	y
0	0	0	0	0
1	0	1	x	y
x	0	x	y	1
y	0	y	1	x

+	0	1	x	y
0	0	1	x	y
1	1	0	y	x
x	x	y	0	1
y	y	x	1	0

2. Let $\phi : F \to F$ be defined as:

$$\phi(0) = 0$$
$$\phi(1) = 1$$
$$\phi(x) = y$$
$$\phi(y) = x$$

To see if this is an automorphism:

(a) By definition, $\phi(0) = 0$ and $\phi(1) = 1$, so $\phi(1_F) = 1_F$.

(b) Because $\phi(0) = 0, \phi(1) = 1$, all cases with 1 and 0 are trivial (addition and multiplication before and after ϕ is identical for the same element). That leaves us with the following cases: $(x, y), (x, x), (y, y)$. Also, $(x, y) = (y, x)$ because fields are abelian. For addition:

$$\phi(a + b) = \phi(a) + \phi(b)$$

$$\phi(x + y) = \phi(1) = 1 = y + x = \phi(x) + \phi(y)$$
$$\phi(x + x) = \phi(2x) = 2y = y + y = \phi(x) + \phi(x)$$
$$\phi(y + y) = \phi(2y) = 2x = x + x = \phi(y) + \phi(y)$$

Hence ϕ is an homomorphism over the additive group. For multiplication:

$$\phi(ab) = \phi(a)\phi(b)$$

$$\phi(xy) = \phi(1) = 1 = yx = \phi(x)\phi(y)$$
$$\phi(xx) = \phi(y) = x = yy = \phi(x)\phi(x)$$
$$\phi(yy) = \phi(x) = y = xx = \phi(y)\phi(y)$$

Hence ϕ is an homomorphism over the multiplicative group.

(c) The map ϕ maps each of the 4 elements from F to 4 elements in F, so the map is clearly both injective and surjective and hence bijective.

Thus, ϕ is a non-identity automorphism of the field F of order 4.

3. In any field there exist exactly 2 identity elements (one multiplicative, one additive). So our field $F' = \{0, 1, a, b\}$, where a, b are the non identity elements in F'. The additive group in this field looks like $F'^{+} = \{0, 1, a, b\}$ with the only possible orders of non-identity elements being $\{2, 4\}$ (Lagrange's Thm). And the multiplicative group in this field looks like $F'^{*} = \{1, a, b\}$ with the only possible order of non-identity elements being $\{3\}$. Knowing these facts and the basic properties of 0 and 1 we can fill some of the additive and multiplicative tables out.

+	0	1	a	b
0	0	1	a	b
1	1			
a	a			
b	b			

.	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a		
b	0	b		

Now, for the additive table we are missing values of $1+1$, $a+a$, $b+b$, $a+b$, $a+1$, $b+1$. The field is abelian so, $a + b = b + a$, $a + 1 = 1 + a$, $b + 1 = 1 + b$. We know that the order of the elements can be either 2, or 4. Assume $\mid 1 \mid = 4$, then under closure of F, $1 + 1$ can be $0, 1, a, b$.

(a) $1+1=0 \implies |\, 1 \,|= 2$, which is a contradiction to our assumption.

(b) $1+1=1 \implies$ that 1 is the identity which is not true because 0 is the additive identity and there can only exist 1 unique identity in a group.

(c) $1+1=a \implies 1+1 = aa^{-1}+aa^{-1} = a^{-1}(2a) = a^{-1}(2(1+1)) = a^{-1}(0) = 0 = a$ which again is not possible because $a, 0$ are distinct elements in the field.

(d) if $1+1=b$ we run into the same problem as above.

So order of 1 cannot be $4 \implies |\, 1 \,|= 2$. Then,

$$\begin{aligned}
&\implies 1+1=0\\
&\implies a+a = a(1+1) = a(0) = 0\\
&\implies b+b = b(1+1) = b(0) = 0
\end{aligned}$$

Up next we should figure out $a+1$:

(a) $a+1=0 \implies a=-1=1 \implies a=1$, which is not possible because $a=1$ are distinct elements in the field.

(b) $a+1=1 \implies a=0$, which is not possible because $a, 0$ are distinct elements in the field.

(c) $a+1=a \implies 0=1$ which again is not possible because $0, 1$ are distinct elements in the field.

(d) $a+1=b$ is the only viable option.

Then,

$$\begin{aligned}
&\implies a+1 = b = 1+a\\
&\implies a+b = a+a+1 = 2a+1 = 0+1 = 0 = b+a\\
&\implies b+1 = a+1+1 = a+0 = a = 1+b
\end{aligned}$$

And, for the multiplicative table we are missing values of a^2, ab, ba, b^2. We know that $ab = ba$ because all fields are abelian. Because the field is closed under multiplication, a^2 can be either $0, 1, a, b$.

(a) $a^2=0 \implies a=0$, which is not possible because $a, 0$ are distinct elements in the field.

(b) $a^2=1 \implies a=1$, which is not possible because $a, 1$ are distinct elements in the field.

(c) $a^2=a \implies a=1$ which again is not possible because $a, 1$ are distinct elements in the field.

(d) $a^2 = b$ which is the only viable option.

Then,

$$\begin{aligned}
&\implies a^2 = b \\
&\implies ab = aa^2 = a^3 = 1 = ba \\
&\implies b^2 = a^2a^2 = a^4 = a^3a = 1a = a
\end{aligned}$$

So finally the tables look like:

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

.	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Now, if we define a homomorphism $\phi : F \to F$ such that:

$$\begin{aligned}
\phi(0) &= 0 \\
\phi(1) &= 1 \\
\phi(x) &= a \\
\phi(y) &= b
\end{aligned}$$

We can see that this homomorphism is obviously bijective because it maps 4 elements from F to 4 elements in F', and both F, F' are groups of order 4. Hence there exists an bijective homomorphism or an isomorphism from $F \to F'$, where F' is any field with 4 distinct elements.