Problem 1. (From Translations and Point Groups to the Full Symmetry Group) Let $E_2$ be the 2-dimensional Euclidean group, i.e., the group of isometries in $\mathbb{R}^2$ under composition.

1. Let $E_2^+$ denote the set of rotations in $E_2$, i.e. the set of isometries of the form $T(x) = \text{Rot}_\theta x + b$, for $\theta \in [0, 2\pi)$ and $b \in \mathbb{R}^2$. Show that $E_2^+$ is a subgroup of $E_2$, and that it is of index 2.

   **Solution.** Recall that to show $E_2^+$ is a subgroup we need to show closure under group operations and presence of inverses. For composition, let $T_1(x) = \text{Rot}_\theta x + b$ and let $T_2(x) = \text{Rot}_\phi + c$. Then $(T_1 \circ T_2)(x) = \text{Rot}_\theta (\text{Rot}_\phi x + c) + b = \text{Rot}_{\theta + \phi} x + (\text{Rot}\theta b + c)$ which is also a rotation in $E_2^+$. To see that the inverses are present, note that if $\phi = -\theta$ and $c = -\text{Rot}_\theta b$ then $T_2 = T_1^{-1}$. Thus $E_2^+$ is a subgroup.

   To show that it has index 2, we note that the only coset of $E_2^+$ is $\text{Ref}_0 \cdot E_2^+$. To see that every member of $E_2$ is in $E_2^+ \cup \text{Ref}_0 \cdot E_2^+$, consider an element $T \in E_2$. Since rotations are already in $E_2^+$ it must be that $T(x) = \text{Ref}_\theta x + b$ for some $\theta$ and $b$. Now note that $\text{Ref}_\theta = \text{Ref}_0 \circ \text{Rot}_{-\theta}$. And so $T(x) = \text{Ref}_0 \circ T_1$ where $T_1(x) = \text{Rot}_{-\theta} x + \text{Ref} \theta b$ in $\text{Ref}_0 \cdot E_2^+$.

2. Let $\text{Isom}(F)^+ = \text{Isom}(F) \cap E_2^+$. Show that either $\text{Isom}(F)^+ = \text{Isom}(F)$ or $\text{Isom}(F)^+$ is a subgroup of $\text{Isom}(F)$ and that it is of index 2. Similarly, for a point $p \in \mathbb{R}^2$, if we define $\text{Point}(F,p)^+ = \text{Point}(F,p) \cap E_2^+$ then $\text{Point}(F,p)^+$ either equals $\text{Point}(F,p)$ or is a subgroup of $\text{Point}(F,p)$ of index 2. (Hint: these statements are have nothing to do with geometry, and
generalize to studying the intersection $H^+$ of arbitrary subgroups $G^+, H$ of a group $G$ such that $[G : G^+] = 2$.

**Solution.** Following the hint, we show that if $H^+ = H \cap G^+$ where $H, G^+ \leq G$ and $[G : G^+] = 2$, then $H = H^+$ or $[H : H^+] = 2$. Assume $H \neq H^+$ and let $h_0 \in H \setminus H^+$. We now show that $H \setminus H^+ = h_0 \cdot H^+$. Consider any $h \in H \setminus H^+$ and let $h^+ = h_0^{-1} h$. We show that $h^+ \in H^+$: To see this, note that since $h_0, h \in H$ we have $h^+ \in H$. But $h_0, h \notin G^+$ and so we have $h_0^{-1} h \in G^+$ since $[G : G^+] = 2$. We thus conclude that $h^+ = h_0^{-1} h \in H \cap G^+ = H^+$ and so $H \setminus H^+ = h_0 H^+$, and so $[H : H^+] = 2$.

To conclude we note that Isom$(F)^+$ is a subgroup of Isom$(F)$ and Point$(F,p)^+$ is a subgroup of Point$(F,p)$. Applying the result of the fist para to $H = Isom(F)$ or $H = Point(F,p)$ yields the desired result.

3. Let Rot$(F) = \{\text{Rot}_\theta : \exists b \text{ s.t. } T(x) = \text{Rot}_\theta x + b \text{ is in Isom}(F)\}$. Show that Rot$(F)$ is a cyclic group generated by Rot$_{\theta^*}$ for the smallest positive value of $\theta^*$ such that Rot$_{\theta^*} \in$ Rot$(F)$.

**Solution.** We note that if Rot$_{\theta_0} \in$ Rot$(F)$ then so is Rot$_{\theta_0 + t_\phi (mod 2\pi)}$ for every pair of integers $s$ and $t$. It follows that the greatest common divisor of $\theta$ and $\phi$ and $2\pi$ is in Rot$(F)$. Since the groups of rotations must be finite, it follows that Rot$(F)$ is generated by a single element Rot$_{\theta^*}$ for some $\theta^*$ dividing $2\pi$.

**Common Errors.** No one answered this question to my satisfaction. :-( . A priori there is no reason why Point$(F,p) = \text{Rot}(F)$ for some $p$. We proved this above, by showing that every rotational isometry (and this is also true for reflections and glide-reflections) actually fixes some point $p$. Then we have that the rotation by $\theta^*$ and shift by $b$, is actually just a rotation about the point $p$, and now, by the notational assumption that $p = 0$, we have that Rot$_{\theta^*} \in$ Point$(F,p)$.

4. Prove that if $p$ is taken to be a point of highest rotational symmetry, then

$$\text{Isom}(F)^+ = \{T_1 \circ T_2 : T_1 \in \text{Trans}(F), T_2 \in \text{Point}(F,p)^+\} \overset{\text{def}}{=} \text{Trans}(F) \circ \text{Point}(F,p)^+.$$  

(For notational simplicity, you may take assume that $p = 0$.)

**Solution.** One direction of the containment is clear: Trans$(F) \circ \text{Point}(F,p)^+ \subseteq \text{Isom}(F)^+$. To see the other direction first we note that the point $p = 0$ of maximal rotational symmetry satisfies Rot$_{\theta^*} \in$ Point$(F,p)^+$. To see this suppose $T_0(x) = \text{Rot}_{\theta^*} x + b$ is in Isom$(F)^+$. Then note that the point $T_0(a) = a$ for $a = (I - \text{Rot}_{\theta^*})^{-1} b$ and so Point$(F,a)$ includes a rotation by angle $\theta^*$. We conclude that a rotation by $\theta^*$ is included in the point group at the point of maximal rotational symmetry. Now consider any isometry $T(x) = \text{Rot}_{\theta^*} x + b$ in Isom$(F)^+$. We must have Rot$_{\theta} = \text{Rot}_{\theta_i}$ for some $i$ and so Rot$_{\theta} \in$ Point$(F,p)^+$. Now (Rot$_{\theta_i}^{-1} \circ T)(x) = x +$ Rot$_{\theta_i}^{-1} \in \text{Trans}(F)$ and so we have $T \in \text{Trans}(F) \circ \text{Point}(F,p)^+$.

**Common Errors.** No one answered this question to my satisfaction. :-( . A priori there is no reason why Point$(F,p) = \text{Rot}(F)$ for some $p$. We proved this above, by showing that every rotational isometry (and this is also true for reflections and glide-reflections) actually fixes some point $p$. Then we have that the rotation by $\theta^*$ and shift by $b$, is actually just a rotation about the point $p$, and now, by the notational assumption that $p = 0$, we have that Rot$_{\theta^*} \in$ Point$(F,p)$.

5. Deduce that if $p$ is a point of highest rotational symmetry, then one of the following cases must hold:

(a) Isom$(F)$ does not contain a reflection or glide-reflection, and Isom$(F) = \text{Trans}(F) \circ \text{Point}(F,p)$.
(b) \(\text{Point}(F,p)\) contains a reflection, and \(\text{Isom}(F) = \text{Trans}(F) \circ \text{Point}(F,p)\).

(c) \(\text{Isom}(F)\) contains a reflection or glide-reflection \(R\), \(\text{Point}(F,p)\) does not contain a reflection, and \(\text{Isom}(F) = (\text{Trans}(F) \circ \text{Point}(F,p)) \cup (\text{Trans}(F) \circ \text{Point}(F,p) \circ R)\).

In particular, we can obtain generators for \(\text{Isom}(F)\) by taking generators for \(\text{Point}(F,p)\) (at most 2 needed), generators for \(\text{Trans}(F)\) (exactly 2 needed), and possibly an additional reflection \(R\).

**Solution.** Note that if \(\text{Isom}(F)\) does not contain a reflection, then \(\text{Isom}(F) = \text{Isom}(F)^+ = \text{Trans}(F) \circ \text{Point}(F,p)^+ \circ \text{Point}(F,p)\), so case (a) is equivalent to asserting “\(\text{Isom}(F)\) does not contain a reflection”. Similarly, case (b) is equivalent to asserting \(\text{Point}(F,p)\) contains a reflection or glide reflection, but \(\text{Point}(F,p)\) does not. Letting this reflection be \(R\) we have \(\text{Isom}(F) = \text{Isom}(F)^+ \cup \text{Isom}(F)^+ \circ R\) (since \([\text{Isom}(F) : \text{Isom}(F)^+] = 2\)). By Part (4) we thus have \(\text{Isom}(F) = (\text{Trans}(F) \circ \text{Point}(F,p)) \cup (\text{Trans}(F) \circ \text{Point}(F,p) \circ R)\).

**Problem 2. (Characteristic and Order of Finite Fields \([AM106]\))**

1. Show that if \(R\) is an integral domain of nonzero characteristic \(p\), then every nonzero element of \(R\) has additive order \(p\).

   **Solution.** For positive integer \(n\) and \(r \in R\) let \(n \cdot r\) denote \(r + r + \cdots + r\) \((n\ times)\). We have \(p \cdot 1 = 0\) and \(p\) is the smallest positive integer such that this happens. Then for every \(r \in R\) we have \(p \cdot r = p \cdot 1 \cdot r = 0 \cdot r = 0\). Now suppose \(q \cdot r = 0\) for some \(0 < q < p\) and \(r \neq 0\) then we have \(q \cdot 1 \cdot r = 0\) and since \(r \neq 0\) it must be that \(q \cdot 1 = 0\) (using the fact that \(R\) is an integral domain) contradicting the minimality of \(p\).

2. Use the classification of finite abelian groups to show that if \(F\) is a finite field of characteristic \(p\), then the order (i.e. size) of \(F\) is \(p^n\) for some \(n \in \mathbb{N}\).

   **Solution.** Let the additive group of \(F\) be isomorphic to \(\mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}\). Then cardinality of \(F\) is \(\prod_{i=1}^k p_i^{n_i}\). If \([F]\) is not a prime power then there exist at least two distinct primes among \(p_1, \ldots, p_k\), so say \(p_1 \neq p_2\). But then \(\mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}\) must have elements of order \(p_1\) as well as \(p_2\) contradicting the conclusion from the first part of this question that every non-zero element in an integral domain has the same order. We conclude that all the \(p_i\)'s are equal and say equal to \(p\). Since some element has order \(p\), we conclude from Part 1 that every element has order \(p\) and so the characteristic of the field is \(p\).

**Problem 3. (Adjoining Square Roots)** Which of the following rings are integral domains? Justify your answers.

1. \([AM106-A]\) \(\mathbb{Z}_{15}[\sqrt{2}]\). (Elements are of the form \((a + b\sqrt{2})\) with \(a, b \in \mathbb{Z}_{15}\), addition defined by \((a + b\sqrt{2}) + (c + d\sqrt{2}) = ((a + c) \mod 15) + ((b + d) \mod 15)\sqrt{2}\), and multiplication defined by \((a + b\sqrt{2})(c + d\sqrt{2}) = ((ac + 2bd) \mod 15) + ((ad + bc) \mod 15)\sqrt{2}\).)

   **Solution.** This is not a field. \(3, 5 \in \mathbb{Z}_{15}[\sqrt{2}]\) are non-zero elements whose product is \(0\).
2. [AM106-A] \( \mathbb{Z}_{11}[\sqrt{2}] \). (Defined similarly to previous item.)

**Solution.** This is a field. See Part (4) for an explanation.

3. [AM106-A] \( \mathbb{Z}_7[\sqrt{2}] \). (Defined similarly to previous item.)

**Solution.** This is not a field. \( 3 + \sqrt{2} \) and \( 3 - \sqrt{2} \) are non-zero elements whose product is \( 9 - 2 = 0 \mod 7 \).

4. [AM206-A] Characterize when \( \mathbb{Z}_n[\sqrt{k}] \) is a field for arbitrary positive integers \( n \) and \( k \). Your characterization should take the form of “\( \mathbb{Z}_n[\sqrt{k}] \) is a field if and only if \( n \) has Property X and the equation ‘\( \cdots = \cdots \)’ (in one variable \( x \)) has no solution in \( \mathbb{Z}_n \).”

**Solution.** \( \mathbb{Z}_n[\sqrt{k}] \) is a field \( \iff \) \( n \) is prime and \( x^2 = k \) has no solutions in \( \mathbb{Z}_n \).

\( \Rightarrow \) If \( n = pq \), then \( p, q \in \mathbb{Z}_n[\sqrt{k}] \) satisfy \( p, q \neq 0 \) and \( pq = 0 \) and so \( \mathbb{Z}_n \) is not an integral domain. If \( n \) is a prime but \( a^2 = k \) for some \( a \in \mathbb{Z}_n \), then we have \( a + \sqrt{k}, a - \sqrt{k} \neq 0 \) (syntactically) but their product \( a^2 - k = 0 \). So again this is not an integral domain.

\( \Leftarrow \) Suppose \( n \) is a prime and \( x^2 = k \) has no solutions in \( \mathbb{Z}_n \). Then we claim \( \mathbb{Z}_n[\sqrt{k}] \) is an integral domain, and since it is finite, it is a field. To verify the claim, suppose \( a + b\sqrt{k}, c + d\sqrt{k} \neq 0 \) but (for contradiction) suppose their product is 0. Then we have \( ac + kbd = 0 \) and \( ad + bc = 0 \).

We divide the analysis into two cases. First, if \( a = 0 \) then we need to have \( bc = 0 \) and \( kbd = 0 \). Since \( k \neq 0 \) this implies \( bc = bd = 0 \) which can happen only if \( b = 0 \) (in which case \( a + b\sqrt{k} = 0 \)) or \( c = d = 0 \) (in which case \( c + d\sqrt{k} = 0 \)) — both of which lead to contradictions. Now suppose \( a \neq 0 \). Then to have \( ad + bc = 0 \) we need \( d = -a^{-1}bc \). Further to have \( ac + kbd = 0 \) we need \( ac - kba^{-1}bc = 0 \). If \( c = 0 \) then \( d = -a^{-1}bc = 0 \) and so \( c + d\sqrt{k} = 0 \) which contradicts our assumption. So \( c \neq 0 \) and if so we must have \( a = ka^{-1}b^2 = 0 \) which implies \( k = (ab^{-1})^2 \) violating the assumption that \( x^2 - k = 0 \) has not solutions in \( \mathbb{Z}_n \).