| AM 106: Applied Algebra | Prof. Madhu Sudan |
|---|---|
| Problem Set 7 | |
| Assigned: Wed. Oct. 25, 2017 | Due: Wed. Nov. 1, 2017 (8:00 AM) |

- You may submit your solutions via assignment page on the canvas website of the course.
- For collaboration and late days policy, see course website at `http://madhu.seas.harvard.edu/courses/Fall2017`
- Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details. Justify your answers except when otherwise specified.

**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. Let $F : \mathbb{R}^2 \to X$ be a 2-dimensional crystal.

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.
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 $[G : G^+] = 2$.)
3. Let $\text{Rot}(F) = \{\text{Rot}_\theta : \exists b \text{ s.t. } T(x) = \text{Rot}_\theta x + b \text{ is in } \text{Isom}(F)\}$. Show that $\text{Rot}(F)$ is a cyclic group generated by $\text{Rot}_{\theta^*}$ for the smallest positive value of $\theta^*$ such that $\text{Rot}_{\theta^*} \in \text{Rot}(F)$.
4. Prove that if $p$ is taken to be a point of highest rotational symmetry, then
$$\text{Isom}(F)^+ = \{T_1 \circ T_2 : T_1 \in \text{Trans}(F), T_2 \in \text{Point}(F, p)^+\} \stackrel{\text{def}}{=} \text{Trans}(F) \circ \text{Point}(F, p)^+.$$
(For notational simplicity, you may take assume that $p = 0$.)
5. Deduce that if $p$ is a point of highest rotational symmetry, then one of the following cases must hold:
   (a) $\text{Isom}(F)$ does not contain a reflection or glide-reflection, and $\text{Isom}(F) = \text{Trans}(F) \circ \text{Point}(F, p)$.
   (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 $R$.

**Problem 2. (Characteristic and Order of Finite Fields)** For a commutative ring $R$ with unity, the characteristic of $R$ is defined as follows. If 1 has finite additive order $p$, then the characteristic of $R$ is defined to be $p$. If 1 has infinite order, then the characteristic of $R$ is defined to be zero.

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

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 $n \in \mathbb{N}$.

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

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

2. $\mathbb{Z}_{11}[\sqrt{2}]$. (Defined similarly to previous item.)

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

4. **(Optional, 0 points)** 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 $\mathbb{Z}_n$."