**Homework #4**

**Plan for next week:** Group actions (§ 4.1-4.3). Start direct and semi-direct products (§ 5.4-5.5).

**Problems, to be submitted by 11:59pm on Thu, October 1st**

**1.** Let $k$ be an algebraically closed field. Let $Y$ be a subset of $k^n$. Let

$$k[Y] = k[x_1, \ldots, x_n]/I(Y).$$

The ring $k[Y]$ can be naturally identified with the ring of polynomial functions from $Y$ to $k$ (with pointwise addition and multiplication). Indeed, every polynomial in $k[x_1, \ldots, x_n]$ naturally defines a function from $Y$ to $k$. Thus, we have a map $ev_Y : k[x_1, \ldots, x_n] \to Func(Y, k)$. By **polynomial functions from $Y$ to $k$** we mean exactly the functions in $\mathrm{Im}\,(ev_Y)$. It is straightforward to check that $ev_Y$ is a ring homomorphism and thus

$$\mathrm{Im}\,(ev_Y) \cong k[x_1, \ldots, x_n]/\mathrm{Ker}\,(ev_Y)$$

Finally, by definition $\mathrm{Ker}\,(ev_Y) = I(Y)$, and thus $k[Y] \cong \mathrm{Im}\,(ev_Y)$.

Let $O(Y)$ be the set of all everywhere defined rational functions on $Y$, that is, all functions $f : Y \to k$ for which there exist polynomials $p, q \in k[x_1, \ldots, x_n]$ s.t. $q$ does not vanish at any point of $Y$ and $f = p/q$ as a function on $Y$. Clearly, $k[Y] \subseteq O(Y)$.

(a) Prove that if $Y$ is an algebraic set, then $O(Y) = k[Y]$. **Hint:** Use the weak Nullstellensatz, version 2.

(b) Let $Y = k^1 \setminus \{0\}$, the affine line with 0 removed. Prove that $k[Y] = k[x]$ (polynomials in one variable) while $O(Y) = k[x, 1/x]$.

(c) Find an algebraic subset $Z$ of $k^2$ such that $k[Z] \cong k[x, 1/x]$. How is $Z$ related to $Y$ from part (b)?

(d) Find a non-algebraic subset $W$ of $k^2$ for which $O(W) = k[W] \cong k[x_1, x_2]$.

**2.** Let $R$ be a commutative ring with 1, and let $n \in \mathbb{N}$. Let $End(R^n)$ be the set of all endomorphism of the additive group $(R^n, +)$.

(a) Define $\iota : Mat_n(R) \to End(R^n)$ by $\iota(A) = (v \mapsto Av)$ (or, in more elementary notation, $(\iota(A)(v)) = Av$ for all $v \in R^n$). Here we think of elements of $R^n$ as column vectors. Prove that $\iota$ is an injective homomorphism of monoids.

(b) Now define $\Phi : End(R^n) \to Mat_n(R)$ as in Lecture 10 (in Lecture 10 we dealt with the special case $R = \mathbb{Z}$, but definition remains the same – $e_i$ is still the element of $R^n$ whose $i^{\text{th}}$ coordinate is 1 and other coordinates are 0). Prove that $\Phi \circ \iota$ is the identity map on $Mat(R^n)$. Deduce that $\Phi$ is always surjective.

(c) By (a) and (b) $\Phi$ is an injective $\iff$ $\Phi$ is an isomorphism $\iff$ $\iota$ is an isomorphism. In Lecture 10 we observed that $\Phi$ is injective for $R = \mathbb{Z}$. Determine (with proof) if $\Phi$ is injective for each of the following rings: (i) $R = \mathbb{Z}_m$ for some $m \in \mathbb{N}$, (ii) $R = \mathbb{Q}$, (iii) $R = \mathbb{Z}[\sqrt{2}]$.

Note that whenever $\Phi$ is an isomorphism, by taking the units on both sides, we get that $\mathrm{Aut}(R^n) \cong GL_n(R)$.

**3.** Let $G$ be a group. For each $g \in G$ let $\iota_g : G \to G$ be the conjugation by $g$, that is, $\iota_g(x) = gxg^{-1}$. Recall that $\iota_g \in \mathrm{Aut}(G)$ for any $g \in G$ and the mapping $\iota : G \to \mathrm{Aut}(G)$ given by $\iota(g) = \iota_g$ is a homomorphism. Elements of the subgroup $\mathrm{Inn}\,(G) = \iota(G)$ of $\mathrm{Aut}(G)$ are called inner automorphisms.

(a) Prove that for any $g \in G$ and $\sigma \in \mathrm{Aut}(G)$ one has $\sigma\iota_g\sigma^{-1} = \iota_{\sigma(g)}$. Deduce that $\mathrm{Inn}\,(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

(b) Let $H$ be a normal subgroup of $G$. Note that for each $g \in G$, the mapping $\iota_g$ restricted to $H$ is an automorphism of $H$. By slight abuse of notation we denote this automorphism of $H$ by $\iota_g$ as well. Prove that $\iota_g$ is an inner automorphism of $H$ if and only if $g \in H \cdot C_G(H)$ where $C_G(H)$ is the centralizer of $H$ in $G$.

**4.** Find the minimal $n$ for which the symmetric group $S_n$ contains an element of order 15 (and prove rigorously why your $n$ is indeed minimal). *Note:* All you need to know about $S_n$ for this problem is stated in Section 1.3 of DF (pp.29-32).

**5.** Let $G = D_8$, the dihedral group of order 8 (that is, the group of isometries of a square). Prove that $|[G,G]| = 2$ and describe $[G,G]$ explicitly without computing every single commutator.

**Index of a subgroup.** If $G$ is a group and $H$ is a subgroup of $G$, the index of $H$ in $G$, denoted by $[G : H]$, is defined to be the cardinality of $G/H$, that is, the number of left cosets of $H$ in $G$. It is not hard to show that the sets $G/H$ (the set of left cosets of $H$) and $H \setminus G$ (the set of right cosets of $H$) always have the same cardinality, so there is no need to introduce "left index" and "right index".

The full statement of Lagrange theorem asserts that if $G$ is a finite group and $H$ is a subgroup of $G$, then $[G : H] = \frac{|G|}{|H|}$ (typically one applies not the full statement but its most useful consequence, namely, that the order of $H$ divides the order of $G$).

**6.** Let $G$ be a group and let $H$ and $K$ be subgroups of $G$ of finite index (note that $G$ is not assumed to be finite).

(a) Assume that $H \subseteq K$. Prove that $[G : H] = [G : K][K : H]$.

(b) Let $m = [G : H]$ and $n = [G : K]$. Prove that

$$\mathrm{LCM}(m, n) \leq [G : H \cap K] \leq mn$$

(where LCM is the least common multiple).

**Hint for (a):** If $A$ is a group and $B$ a subgroup of $A$, a subset $S$ of $A$ is called a left transversal of $B$ in $A$ if $S$ contains precisely one element from each left coset of $B$ (an alternative name for a transversal is a system of left coset representatives). Let $\{g_1, \ldots, g_r\}$ be a left transversal of $K$ in $G$ and $\{k_1, \ldots, k_s\}$ a left transversal of $H$ in $K$. Prove that $\{g_i k_j\}_{1 \leq i \leq r, 1 \leq j \leq s}$ is a left transversal for $H$ in $G$. Recall that if $B$ is a subgroup of a group $G$, then $xB = yB \iff x^{-1}y \in B$ for $x, y \in G$.