Math 581 Problem Set 7

1. Let $f(x) \in \mathbb{Q}[x]$ be a polynomial. A ring isomorphism $\phi : R \to R$ is called an automorphism.
(a) Let $\phi : \mathbb{C} \to \mathbb{C}$ be a ring homomorphism so that $\phi(a) = a$ for all $a \in \mathbb{Q}$. Prove that if $\alpha \in \mathbb{C}$ is a root of $f(x)$, then $\phi(\alpha)$ is a root of $f(x)$. In particular, this shows if $\phi : K \to K$ is a ring homomorphism with $K \subseteq \mathbb{C}$, then if $\alpha \in K$ is a root of $f(x) \in \mathbb{Q}$, then $\phi(\alpha)$ must also be a root of $f(x)$.
(b) Use part (a) to show that if $\phi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]$ is an isomorphism so that $\phi(a) = a$ for all $a \in \mathbb{Q}$ (we normally say ϕ fixes $\mathbb{Q}$), then ϕ is either the identity map sending $a + b\sqrt{2}$ to $a + b\sqrt{2}$ or the "conjugation map" sending $a + b\sqrt{2}$ to $a - b\sqrt{2}$.
(c) Show that the set of $\phi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]$ that fix $\mathbb{Q}$ is a group of order 2.
(Note here that $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$ and the order of the group of ring homomorphisms fixing $\mathbb{Q}$ is of order 2! We write $\mathrm{Gal}(\mathbb{Q}[\sqrt{2}]/\mathbb{Q})$ for the group of automorphisms of $\mathbb{Q}[\sqrt{2}]$ that fix $\mathbb{Q}$. It is the "Galois group" of the field.)

2. **(a)** Let G and H be groups. Prove that $G \times H$ is a group. If G and H are finite, then $|G \times H| = |G||H|$.
(b) Consider the additive group $\mathbb{Z}/2\mathbb{Z}$ and the group of units $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Write out the operation table for the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}[i]^\times$.

3. Decide if the following sets are groups under the given operation $*$.
(a) $G = \{2^x | x \in \mathbb{Q}\}; a * b = ab$
(b) $G = \{n \in \mathbb{Z} | n \equiv 1 (\mathrm{mod}\, 5)\}; a * b = ab$
(c) $G = \{x \in \mathbb{R} | x \neq -1\}; a * b = ab + a + b$

4. Describe the group of symmetries for a regular pentagon. Find the order of each element in the group you find. Is your group S_5?

5. Let G be a group. The *center* $Z(G)$ of G is defined to be

$$Z(G) = \{a \in G : ag = ga \text{ for every } g \in G\}.$$

(a) Prove that $Z(G)$ is a subgroup of G.
(b) Find $Z(\mathrm{GL}_2(\mathbb{R}))$.

6. Let $G = \langle a \rangle$ be a cyclic group of order n.
(a) If H is a subgroup of G, show that $|H|$ divides n.
(b) If k is a positive divisor of n, prove that G has a unique subgroup of

order k.

7. **(a)** Let G be an abelian group of order mn where $\gcd(m, n) = 1$. Assume G contains an element a of order m and an element b of order n. Prove that G is cyclic with generator ab.
(b) Prove that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic if and only if $\gcd(m, n) = 1$.

8. Let G be an abelian group and n a fixed positive integer.
(a) Prove that $H = \{a \in G | a^n = e\}$ is a subgroup of G.
(b) Show that part (a) may be false if we do not assume G is abelian. You may want to look at the group S_3 to see this.