Math 581 Problem Set 7 Solutions

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 $f(x)$.

Proof: Write $f(x) = a_n x^n + \cdots + a_1 x + a_0$ with $a_i \in \mathbb{Q}$. Since α is a root of $f(x)$, we have $f(\alpha) = 0$. Using that ϕ is an homomorphism and that $\phi(a) = a$ for every $a \in \mathbb{Q}$, we have

$$\begin{aligned} 0 &= \phi(0) \\ &= \phi(a_n\alpha^n + \cdots a_1\alpha + a_0) \\ &= a_n\phi(\alpha)^n + \cdots a_1\phi(\alpha) + a_0. \end{aligned}$$

Thus, $\phi(\alpha)$ is a root of $f(x)$ as well. ■

(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 $a - b\sqrt{2}$.

Proof: Let ϕ be such a homomorphism. Recall that elements of $\mathbb{Q}[\sqrt{2}]$ are of the form $a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$. Thus, since ϕ is a homomorphism and fixes $\mathbb{Q}$, we have $\phi(a + b\sqrt{2}) = a + b\phi(\sqrt{2})$. Thus, the map ϕ is completely determined by what it does to $\sqrt{2}$. However, by part (a) with $f(x) = x^2 - 2$, we see that $\phi(\sqrt{2}) = \pm\sqrt{2}$. Thus we have the result. ■

(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.)

Proof: If we write e for the identity and ϕ for the map sending $a + b\sqrt{2}$ to $a - b\sqrt{2}$, we see that $\phi^2 = e$. It is easy to see this is a group of order two now, in fact, it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. ■

2. (a) Let G and H be groups. Prove that $G \times H$ is a group. If G and H are finite, then $|G \times H| = |G||H|$.

Proof: Let $\star$ be the group operation on G and $*$ the group operation on H. Define a group operation $\cdot$ on $G \times H$ by $(a, b) \cdot (c, d) = (a \star c, b * d)$. Note that $G \times H$ is clearly closed under this operation since G and H are groups and hence closed. It also follows we have associativity because we have it for $\star$ and $*$. Observe that (e_G, e_H) is the identity element of $G \times H$ under the operation $\cdot$. Let $(a, b) \in G \times H$. It is then easy to see that (a^{-1}, b^{-1}) is the inverse of (a, b). Thus, $G \times H$ is a group. If G and H are finite, then the fact that $|G \times H| = |G||H|$ follows from the corresponding fact about sets. ■

(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 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}[i]^\times$.

$*$	(0,1)	(0,-1)	(0, i)	(0 , -i)	(1,1)	(1,-1)	(1,i)	(1,-i)
(0,1)	(0,1)	(0,-1)	(0, i)	(0 , -i)	(1,1)	(1,-1)	(1,i)	(1,-i)
(0,-1)	(0,-1)	(0,1)	(0, -i)	(0 , i)	(1,-1)	(1,1)	(1,-i)	(1,i)
(0,i)	(0,i)	(0,-i)	(0, -1)	(0 , 1)	(1,i)	(1,-i)	(1,-1)	(1,1)
(0,-i)	(0,-i)	(0,i)	(0, 1)	(0 , -1)	(1,-i)	(1,i)	(1,1)	(1,-1)
(1,1)	(1,1)	(1,-1)	(1, i)	(1 , -i)	(0,1)	(0,-1)	(0,i)	(0,-i)
(1,-1)	(1,-1)	(1,1)	(1, -i)	(1 , i)	(0,-1)	(0,1)	(0,-i)	(0,i)
(1,i)	(1,i)	(1,-i)	(1, -1)	(1 , 1)	(0,i)	(0,-i)	(0,-1)	(0,1)
(1,-i)	(1,-i)	(1,i)	(1, 1)	(1 , -1)	(0,-i)	(0,i)	(0,1)	(0,-1)

3. Decide if the following sets are groups under the given operation $*$.
(a) $G = \{2^x | x \in \mathbb{Q}\}; a * b = ab$

This is a group. Let 2^x and 2^y be in G. Observe that $2^x * 2^y = 2^{x+y} \in G$. Associativity is clear. The identity element is $2^0 = 1$. Finally, the inverse of 2^x is $2^{-x} \in G$.

(b) $G = \{n \in \mathbb{Z} | n \equiv 1 (\mathrm{mod}\, 5)\}; a * b = ab$

This is not a group as we do not have inverses. For example, $6 \in G$ but 6^{-1} is not even in $\mathbb{Z}$, let alone in G.

(c) $G = \{x \in \mathbb{R} | x \neq -1\}; a * b = ab + a + b$

This is a group. It is closed: suppose $a * b = -1$, i.e., $ab + a + b = -1$.

Thus, $a(b+1) = -(1+b)$. Since $b \neq -1$, we have $a = -1$, a contradiction. Thus G is closed under $*$. The associativity follows: $(a*b)*c = (ab+a+b)*c = abc+ac+bc+ab+a+b+c = a*(b*c)$. The identity element is 0 and the inverse of a is $-\dfrac{a}{1+a}$, which makes sense since $a \neq -1$.

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?

The group of symmetries is what is known as a dihedral group. For a regular n-gon, the group of symmetries is written D_{2n} and has order $2n$. The elements are given by $\{e, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$ where r is a "rotation" and s is a reflection. It does not matter which rotation or reflection you pick, you will get an isomorphic group. Make sure that your "hands on" way of describing this group matches up with the more general notion given here.

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.

Proof: Note that $e_G a = a = a e_G$ for all $a \in G$, so $e_G \in Z(G)$. Let $a, b \in Z(G)$. To see $ab \in Z(G)$, observe that $(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab)$ for all $g \in G$ as required. Now let $g \in G$ and we show $a^{-1} \in Z(G)$ if $a \in Z(G)$. Observe that since $a \in Z(G)$, $ag^{-1} = g^{-1}a$. Taking inverses of both sides we obtain $(ag^{-1}) = (g^{-1}a)$, i.e., $ga^{-1} = a^{-1}g$, as desired. Thus $Z(G)$ is a subgroup of G. ■

(b) Find $Z(\mathrm{GL}_2(\mathbb{R}))$.

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(\mathrm{GL}_2(\mathbb{R}))$. Since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$, we can use this to see that $a = d$ and $c = 0$. Similarly, we can use the matrix $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ to get $b = 0$ as well. Thus,

$$Z(\mathrm{GL}_2(\mathbb{R})) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} | a \in \mathbb{R} \right\}.$$

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.

Proof: We know that H must be a cyclic group, so there exists $k \in \mathbb{N}$ such that $H = \langle a^k \rangle$. We know from class that the order of a^k is precisely n/k, thus, the order of H is n/k, so a divisor of n. ■

(b) If k is a positive divisor of n, prove that G has a unique subgroup of order k.

Proof: The subgroup of order k is the subgroup $H = \langle a^{n/k} \rangle$. It is clear this group has order k and is a subgroup. Say $mk = n$. Now suppose we have another subgroup of order k, say H. Since H is a subgroup of a cyclic group it must itself be cyclic, say $H = \langle a^l \rangle$. If we can show that $a^l \in \langle a^m \rangle$, then we will have $H \subset \langle a^m \rangle$ and since they both have k elements they will be equal. So it remains only to show that $m|l$. Use the division algorithm to write $l = mq + r$ with $0 \leq r < m$. Then we have $a^l = a^{mq+r} = (a^m)^q a^r$. Raising both sides to the k we get $a^{rk} = e$. However, $r < m$ so $rk < mk = n$. This is a contradiction to the fact that a has order n unless $r = 0$. Thus, $m|l$. ■

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.

Proof: Consider the subgroup $H = \langle ab \rangle$ inside of G. Since G is abelian we are able to conclude that $(ab)^{mn} = e$. To see that $G = H$ we need only show that the elements $ab, (ab)^2, \ldots, (ab)^{mn}$ are all distinct. This is equivalent to showing that $(ab)^j \neq e$ for $0 < j < mn$. Suppose there exists a j with $0 < j < mn$ and $(ab)^j = e$. In particular, we have $a^j = b^{-j}$. Observe that we have $e = b^{-jn} = (b^{-j})^n = (a^j)^n$, i.e., $a^{jn} = e$. Thus, it must be that $m|jn$. However, since $\gcd(m, n) = 1$, it must in fact be that $m|j$. A similar argument gives $n|j$. Hence, the least common multiple of m and n, which in this case is mn, must divide j. This is a contradiction to $0 < j < mn$, thus we have $G = H$ as claimed. ■

(b) Prove that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic if and only if $\gcd(m, n) = 1$.

Proof: If $\gcd(m, n) = 1$, then we apply part (a) with $G = \mathbb{Z}/m\mathbb{Z}$ and $H = \mathbb{Z}/n\mathbb{Z}$ to obtain the result. Now suppose $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic and $\gcd(m, n) = d$. Let (a, b) be a generator of this group (in fact, one could

take $(1,1)$.) Observe then that $\frac{mn}{d}(1,1) = \left(\left(\frac{n}{d}m, \frac{m}{d}n\right)\right. = (0,0)$. However, if $d > 1$ then we will end up with only $\frac{mn}{d}$ elements in G, a contradiction. Thus it must be that $d = 1$. ■

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.

Proof: Note that H is nonempty because $e \in H$. Suppose $a, b \in H$. Using that G is abelian we have $(ab)^n = a^n b^n = e \cdot e = e$, so $ab \in H$. Similarly, if $a \in H$, then $(a^{-1})^n = a^{-n} = (a^n)^{-1} = e^{-1} = e$. Thus, H 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.

Consider the group S_3 and $n = 2$. Then $H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$.
However, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, which is not in H.