Proof Portfolio (Draft1)

Student: Ryan Baldwin, `rbaldwi2@swarthmore.edu`

Professor: Dr. Hsu

1 Proof By Contradiction (Contradiction Removed):

1.1 Assessment 3, question 3 (b):

Determine whether the given rings are isomorphic. Be sure to explain.

$$\mathbb{Z} \quad \text{and} \quad \frac{\mathbb{Z}[x]}{(2x-1)}$$

Proof. Notice that in the ring $\mathbb{Z}[x]/(2x-1)$, the ideal $\overline{2x-1} = \bar{0}$ implies that $\overline{2x} = \bar{1}$, or equivalently, $2x = 1$. In $\mathbb{Z}$, the ideal is generated by (1). The ideal (1) sends all integers to zero, but the ideal $(2x-1)$ only sends integer multiples of 2 to zero.

Since there is no bijective correspondence between the two ideals of each respective ring, there cannot be an isomorphism between $\mathbb{Z}[x]/(2x-1)$ and $\mathbb{Z}$.

Therefore, we conclude that the two rings are not isomorphic.

$\square$

2 Proof With Significant Edits:

2.1 Lemma:

If m is an invertible element and H and K are sets, then $mH \cap mK = m(H \cap K)$.

Proof. We will show, through double containment, that $mH \cap mK = m(H \cap K)$.

First containment $m(H \cap K) \subseteq mH \cap mK$**:**

Let $w \in m(H \cap K)$. Then, w can always be expressed as an element of either set. Thus, the subset holds true.

Second Containment $mH \cap mK \subseteq m(H \cap K)$**:**

Let $z \in mH \cap mK$. Then, $z = mh = mk$ for some $h \in H$ and for some $k \in K$. Left multiplying $mh = mk$ by m^{-1} yields $h = k$. This implies that h lies in both H and K. Hence, z is an element of $m(H \cap K)$, and the subset holds true.

Thus, we have indeed proven the lemma to be true. □

2.2 Michael Artin's Algebra, Chapter 2, question 10.2 (a) and (b):

Let H and K be subgroups of a group G.

- **(a)** Prove that the intersection $xH \cap yK$ of two cosets of H and K is either empty or else is a coset of the subgroup $H \cap K$.
- **(b)** Prove that if H and K have finite index in G then $H \cap K$ also has finite index in G.

Proof. (a) Let xH and yK be two cosets of H and K respectively. We want to show that the intersection of these two cosets is either empty or a coset of the subgroup $H \cap K$.

Consider the case where the cosets have no overlapping elements. Then, $xH \cap yK = \emptyset$.

Now let us consider the case where the intersection of the two cosets is nonempty. Let a be an element that lies in $xH \cap yH$. Because it is an element of the intersection, $a = xh = yk$ for some $h \in H$ and $k \in K$. Furthmore, since cosets are equivalent up to their representatives, aH is equivalent to the coset xH, and aK is equivalent to the coset yK. Thus,

$$xH \cap yK = aH \cap aK.$$

Applying **Lemma 2.1** to the intersection of the two cosets, we see that

$$xH \cap yK = aH \cap aK = a(H \cap K), \quad \text{a coset of} \quad H \cap K. \tag{1}$$

Therefore, $xH \cap yH$ is either empty or a coset of the subgroup $H \cap K$. □

Proof. (b)

Let $[G : H] = n$ and let $[G : K] = m$, where n and m are integers.

Equation (1) from part (a) implies that the intersection of two cosets each multiplied by the same representative a is equal to the intersection of the two cosets represented by a. This equation defines a relation between the coset of $H \cap K$ and the cosets of H and K, so long as they share the same representative (i.e. $aH \cap aK = a(H \cap K)$).

Without loss of generality, suppose $H \subset K \subset G$. Then, by **Proposition 2.8.14**,

$$[G : H] = [G : K][G : H].$$

Furthermore, since $1(H \cap K) = 1H \cap 1K$, it follows that the number of cosets of $1(H \cap K)$ will not exceed the product of the number of cosets in H and K respectively. Thus, we see that

$$[G : H \cap K] \leq [G : K][G : H] = m \cdot n.$$

Therefore, $H \cap K$ has finite index in G. □

3 Proudest Proof:

3.1 Artin Chapter 2: Additional Problem 1:

Show that a group with no proper nontrivial subgroups is cyclic

Proof. Let G be a group. To prove this claim, we will consider two cases that cover all possible orders of a group G.

Case I: $|G| = 1$.

Consider the case where the order of G is 1. The only element of G must be the identity element e, which can serve as a generator for the whole group. Since the order of G is 1, $|\langle e \rangle| = 1$. Thus, $\langle e \rangle$ is a cyclic group.

Case II: $|G| \geq 2$.

Furthermore, consider the case where the order of G is greater than or equal to 2. Let a be a nontrivial element of G and note that $\langle a \rangle$ is a group of order less than or equal to G. Because we have assumed that the group has no proper nontrivial subgroups, a must serve as a generator for the entire group G. Since the order of $\langle a \rangle$ is finite, G must be cyclic.

Therefore, a group with no proper nontrivial subgroups is cyclic. $\square$

4 Bonus Proof:

4.1 Assessment 3, question 3 (d):

Determine whether the given rings are isomorphic. Be sure to explain.

$$\frac{\mathbb{R}[x]}{(x^2+1)} \quad \text{and} \quad \frac{\mathbb{R}[x]}{(3x^2+5)}$$

We note that the roots of the polynomial (x^2+1) are $\pm i$. Consider the following map:

$$\begin{array}{rcl} \varphi : \frac{\mathbb{R}[x]}{(x^2+1)} & \rightarrow & \mathbb{R}[i] \\ x & \mapsto & i \end{array}$$

We note that φ is a ring homomorphism. We see that φ is surjective, since the image of x is i. Furthermore, since the principal ideal is the only ideal in $\mathbb{R}[x]$ that maps to 0, the kernel of φ is trivial and the map φ is injective. Thus, φ is an isomorphism, and $\frac{\mathbb{R}[x]}{(x^2+1)} \cong \mathbb{R}[i]$.

Similarly, the roots of the polynomial $(3x^2+5)$ are $\pm i\sqrt{\frac{5}{3}}$. Let $\alpha = \sqrt{\frac{5}{3}}$, and consider the following map:

$$\begin{array}{rcl} \phi : \frac{\mathbb{R}[x]}{(3x^2+5)} & \rightarrow & \mathbb{R}[\alpha i] \\ x & \mapsto & \alpha i \end{array}$$

Notice that ϕ is also a ring homomorphism. Observe that ϕ is surjective, since the image of x is αi. And because the kernel of ϕ is trivial, ϕ must be injective. Thus, ϕ is an isomorphism, and $\frac{\mathbb{R}[x]}{(3x^2+5)} \cong \mathbb{R}[\alpha i]$.

Since φ and ϕ are both isomorphisms, we want to show whether or not the rings $\mathbb{R}[i]$ and $\mathbb{R}[\alpha i]$ are isomorphic. Recall that the evaluation of real polynomials at a complex number yields a ring homomorphism to the complex numbers (Artin 11.3). This homomorphism is defined by the following map:

$$\begin{array}{rcl} \psi : \mathbb{R}[x] & \rightarrow & \mathbb{C} \\ x & \mapsto & i \end{array}$$

We see that ψ is surjective, since the image of x is i, and ψ is injective, since the kernel of ψ is trivial. Thus, there is an isomorphism between the ring $\mathbb{R}[x]$ and $\mathbb{C}$, and consequently $R[i] \cong \mathbb{C}$ and $R[\alpha i] \cong \mathbb{C}$. This implies that $\mathbb{R}[i] \cong \mathbb{R}[\alpha i]$.

Therefore, these two rings are indeed isomorphic.