Name: Huize Shi - A92122910
Discussion: A04
Homework: 4

---

1. Prove that $\mathbb{Q}[x]/\langle x^2-2\rangle \simeq \mathbb{Q}[\sqrt{2}]$.

   Define ring homomorphism: $f : \mathbb{Q}[x] \mapsto \mathbb{Q}[\sqrt{2}]$ by evaluation map $f(g(x)) = g(\sqrt{2})$. We have already proven in class that evalution maps are homomorphic.

   Show $\langle x^2-2\rangle = ker\ f$:
   First show $\langle x^2-2\rangle \subseteq ker\ f$:

$$\begin{aligned} f(x^2-2) &= (\sqrt{2})^2 - 2 \\ &= 2-2 \\ &= 0 \end{aligned}$$

   Hence shown $x^2-2 \in ker\ f$, $\langle x^2-2\rangle \subseteq ker\ f$

   Then show $ker\ f \subseteq \langle x^2-2\rangle$:
   Given generic value in $ker\ f$, $g(x)$, show that it is in (divisible by) $\langle x^2-2\rangle$.

$$\begin{aligned} g(x) \in ker\ f &\Rightarrow g(x) = q(x)\cdot(x^2-2) + r(x) \text{ where } deg(r) \leq 1 \\ &\Rightarrow r(x) = l_1 x + l_2 \end{aligned}$$

   Show that r is 0 if it is in the kernel.

$$f(r(x)) = l_1\sqrt{2} + l_2 = 0 \Rightarrow l_1 = l_2 = 0$$

   This implication is true since otherwise l_2 will need to be a multiple of $\sqrt{2}$ which is not in $\mathbb{Q}$. Hence shown $x^2-2 \mid ker\ f$, $ker\ f \subseteq \langle x^2-2\rangle$.

   Hence shown $ker\ f = \langle x^2-2\rangle$.

   f is surjective: Given any $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, $f(a+bx) = a+b\sqrt{2}$.
   By 1^{st} isomorphism theorem, $\mathbb{Q}[x]/\langle x^2-2\rangle \simeq \mathbb{Q}[\sqrt{2}]$.

2. Prove that $\mathbb{Z}[i]/\langle 2+i\rangle \simeq \mathbb{Z}/5\mathbb{Z}$.

Define ring homomorphism: $f : \mathbb{Z}[i] \mapsto \mathbb{Z}/_{5\mathbb{Z}}$ by $f(a+bi) = a - 2b$.

$$\begin{aligned} f((a+bi)+(c+di)) &= f((a+c)+(b+d)i) \\ &= (a+c) - 2(b+d) \\ &= a - 2b + c - 2d \\ &= f(a+bi) + f(c+di) \end{aligned}$$

$$\begin{aligned} f((a+bi)\cdot(c+di)) &\stackrel{?}{=} f(a+bi)\cdot f(c+di) \\ f((ac-bd)+(ad+bc)i) &\stackrel{?}{=} (a-2b)(c-2d) \\ (ac-bd) - 2(ad+bc) &= (ac-bd) - 2(ad+bc) \end{aligned}$$

Show $\langle 2+i \rangle = ker\ f$**:**
First show $\langle 2+i \rangle \subseteq ker\ f$:

$$\begin{aligned} f(2+i) &= 2 - 2 \\ &= 0 \end{aligned}$$

Hence shown $2 + i \in ker\ f$, $\langle 2+i \rangle \subseteq ker\ f$

Then show $ker\ f \subseteq \langle 2+i \rangle$:
Given generic element in $ker\ f$, $a + bi$:

$$\begin{aligned} \frac{a+bi}{2+i} &= a' + b'i = (q_1 + e_1) + (q_2 + e_2)i \text{ where } q \in \mathbb{Z},\ |e| < \frac{1}{2} \\ &= (q_1 + q_2 i) + (e_1 + e_2 i) \\ a + bi &= (2+i)(q_1 + q_2 i) + (2+i)(e_1 + e_2 i) \end{aligned}$$

Let $r = r_1 + r_2 i = (2+i)(e_1 + e_2 i)$.

$$\begin{aligned} |r|^2 &= |2+i|^2 \cdot |e_1 + e_2 i|^2 \\ &= 5 \cdot (e_1^2 + e_2^2) \le 2.5 \\ |r|^2 &= r_1^2 + r_2^2 \le 2.5 \Rightarrow |r_i| \le 1 \end{aligned}$$

Since $r \in ker\ f$, $f(r) = r_1 - 2r_2 + 5\mathbb{Z}$. $5 \mid r_1 - 2r_2$, and $r_i \in -1, 0, 1 \Rightarrow r_1 = r_2 = 0 \Rightarrow r = 0$.

f **is surjective:** Given any element in $\mathbb{Z}/_{5\mathbb{Z}}$, $a + 5\mathbb{Z}$, $f(a + 0i) = a + 5\mathbb{Z}$. Hence f is surjective.

By 1^{st} isomorphism theorem, $\mathbb{Z}[i]/_{\langle 2+i \rangle} \simeq \mathbb{Z}/_{5\mathbb{Z}}$

3. Suppose $m, n \in \mathbb{Z}^{\ge 2}$ and $gcd(m,n) = 1$. Prove that

$$\mathbb{Z}/_{mn\mathbb{Z}} \simeq \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}$$

Ring homomorphism:

$$f : \mathbb{Z} \mapsto {}^{\mathbb{Z}}\!/_{m\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$$
$$f(z) = (z + m\mathbb{Z}, z + n\mathbb{Z})$$

$$\begin{aligned} f(z+z) &= (2z + m\mathbb{Z}, 2z + n\mathbb{Z}) \\ &= (z + m\mathbb{Z}, z + n\mathbb{Z}) + (z + m\mathbb{Z}, z + n\mathbb{Z}) \\ &= f(z) + f(z) \end{aligned}$$

$$\begin{aligned} f(zz) &= (zz + m\mathbb{Z}, zz + n\mathbb{Z}) \\ &= (z + m\mathbb{Z}, z + n\mathbb{Z})(z + m\mathbb{Z}, z + n\mathbb{Z}) \\ &= f(z)f(z) \end{aligned}$$

Show $ker\ f = mn\mathbb{Z}$
First show $mn\mathbb{Z} \subseteq ker\ f$:

$$\begin{aligned} f(mnz) &= (mnz + m\mathbb{Z}, mnz + n\mathbb{Z}) \\ &= (0, 0) \end{aligned}$$

Then show $ker\ f \subseteq mn\mathbb{Z}$:

$$\begin{aligned} f(z) &= (0, 0) \\ (z + m\mathbb{Z}, z + n\mathbb{Z}) &= 0 \end{aligned}$$

This implies $m \mid z$, $n \mid z$. Since $gcd(m, n) = 1$, this implies $z \in mn\mathbb{Z}$
Hence shown $ker\ f = mn\mathbb{Z}$.

4. Prove that ${}^{\mathbb{Z}[x]}\!/_{n\mathbb{Z}[x]} \simeq \mathbb{Z}_n[x]$.

$$f : \mathbb{Z}[x] \mapsto \mathbb{Z}_n[x]$$
$$f\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} a_i x^i + n\mathbb{Z}$$

f is clearly surjective and homomorphic since it sends every element to their corresponding elements mod n (multiplication and addition maps with mod n applied before or after does not matter).

Show $ker\ f = n\mathbb{Z}[x]$**:** Showing subsets for both directions.
First show $n\mathbb{Z}[x] \subseteq ker\ f$:

$$f(na_ix^i) = na_ix^i + 5\mathbb{Z} \overset{n}{\equiv} 0$$

Then show $ker\ f \subseteq n\mathbb{Z}[x]$. Since f maps g to g where all coefficients are remainders divided by n, $g(x) \in ker\ f$ implies that the coefficients of $g(x)$ must be 0 $mod\ n$. This immplies that the coefficients of the kernel of f is in $n\mathbb{Z}$. This means that the kernel of f is in $n\mathbb{Z}[x]$.

Show that f **is surjective:** This is true by the definition of f:

$$f\left(\sum_{i=0}^{n} a_ix^i\right) = \sum_{i=0}^{n} a_ix^i + n\mathbb{Z}$$
$$\sum_{i=0}^{n} a_ix^i + n\mathbb{Z} = \mathbb{Z}_n[x]$$

By 1^{st} isomorphism theorem, $\mathbb{Z}[x]/n\mathbb{Z}[x] \simeq \mathbb{Z}_n[x]$.

5. Prove that $\mathbb{Q}[x]/\langle x^2 - 2x + 6\rangle \simeq \{c_0 + c_1A \mid c_0, c_1 \in \mathbb{Q}\}$, where $A = \begin{bmatrix} 0 & -6 \\ 1 & 2 \end{bmatrix}$.

$$\phi_A : \mathbb{Q}[x] \mapsto M_2(\mathbb{Q})$$
$$\phi_A\left(\sum_{i=0}^{n} a_ix^i\right) = \sum_{i=0}^{n} a_iA^i$$

Show $\langle x^2 - 2x + 6\rangle = ker\ \phi_A$**:**
First show that $\langle x^2 - 2x + 6\rangle \subseteq ker\ \phi_A$:

$$\begin{aligned} \phi_A(x^2 - 2x + 6) &= A^2 - 2A + 6 \\ &= \begin{bmatrix} -6 & -12 \\ 2 & -2 \end{bmatrix} - \begin{bmatrix} 0 & -12 \\ 2 & 4 \end{bmatrix} + \begin{bmatrix} 6 & 0 \\ 0 & 6 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \end{aligned}$$

Then show that $ker\ \phi_A \subseteq \langle x^2 - 2x + 6\rangle$:

$$\begin{aligned} f(x) \in ker\ \phi_A &\Rightarrow f(x) = p(x)(x^2 - 2x + 6) + r(x) \text{ where } deg(r) \le 1 \\ &\Rightarrow r(x) = l_1x + l_2 \\ &\Rightarrow l_1A + l_2 = 0 \\ &\Rightarrow A = l_2l_1^{-1} \text{ However, } l \text{ might not be invertable} \\ &\Rightarrow l_1 = l_2 = 0 \end{aligned}$$

Show that ϕ_A is surjective: Show $Im\ \phi_A = \{c_0 + c_1 A \mid c_0, c_1 \in \mathbb{Q}\}$
Show $\sum_{i=0}^{n} a_i x^i \subseteq \{c_0 + c_1 A \mid c_0, c_1 \in \mathbb{Q}\}$
Since $\phi_A(x^2 - 2x + 6) = A^2 - 2A + 6 = 0 \Rightarrow A^2 = 2A - 6$, therefore we can reduce degree from two to one. For equation of any degree, we can reduce the degree to first degree which is in $\{c_0 + c_1 A \mid c_0, c_1 \in \mathbb{Q}\}$. This means that ϕ_A is surjective.

By 1^{st} isomorphism theorem, $\mathbb{Q}[x] \big/ \langle x^2 - 2x + 6 \rangle \simeq \{c_0 + c_1 A \mid c_0, c_1 \in \mathbb{Q}\}$.