Math 103B Homework 4 Solution

Haiyu Huang
April 28, 2018

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

Proof. Consider $\phi : \mathbb{Q}[x] \to \mathbb{C}$ given by $f \mapsto f(\sqrt{2})$.

- ϕ is a ring homomorphism:
$$\phi(f)+\phi(g) = f(\sqrt{2})+g(\sqrt{2}) = (f+g)(\sqrt{2}) = \phi(f+g)$$
and
$$\phi(f)\phi(g) = f(\sqrt{2})g(\sqrt{2}) = (fg)(\sqrt{2}) = \phi(fg).$$

- $\mathrm{Im}\phi = \mathbb{Q}[\sqrt{2}]$: for every $f(x) = \sum_{i=0}^m a_i x^i \in \mathbb{Q}[x]$, $f(\sqrt{2}) = \sum_{i=0}^m a_i(\sqrt{2})^i \in \mathbb{Q}[\sqrt{2}]$, so $\mathrm{Im}\phi \subset \mathbb{Q}[\sqrt{2}]$; for every $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, $\phi(a+bx) = a+b\sqrt{2}$ implies $\mathrm{Im}\phi \supset \mathbb{Q}[\sqrt{2}]$.

- $\ker\phi = \langle x^2-2\rangle$: $\phi(x^2-2) = (\sqrt{2})^2-2 = 0$ implies $\langle x^2-2\rangle \subset \ker\phi$. Let $f(x) \in \ker\phi$. By long division, $\exists q(x), r(x) \in \mathbb{Q}[x]$ such that $f(x) = q(x)(x^2-2)+r(x)$, where $\deg r < \deg(x^2-2) = 2$. So $\phi(r) = \phi(f) = 0$. Suppose $r(x) = a+bx \in \mathbb{Q}[x]$ for $a, b \in \mathbb{Q}$. Then $\phi(r) = a+b\sqrt{2} = 0$ implies $a = b = 0$. Thus, $r = 0$ and $f(x) \in \langle x^2-2\rangle$. It follows that $\ker\phi \subset \langle x^2-2\rangle$.

The conclusion follows by the first isomorphism theorem. ■

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

Proof. Let $\phi : \mathbb{Z}[i] \to \mathbb{Z}/5\mathbb{Z}$ be given by $a+bi \mapsto a+3b+5\mathbb{Z}$.

- ϕ is a ring homomorphism:
$$\begin{aligned}\phi(a+bi)+\phi(c+di) &= (a+3b+5\mathbb{Z})+(c+3d+5\mathbb{Z})\\ &= (a+c)+3(b+d)+5\mathbb{Z}\\ &= \phi(a+c+(b+d)i)\\ &= \phi((a+bi)+(c+di))\end{aligned}$$
and
$$\begin{aligned}\phi(a+bi)\phi(c+di) &= (a+3b+5\mathbb{Z})\cdot(c+3d+5\mathbb{Z})\\ &= ac+9bd+3ad+3bc+5\mathbb{Z}\\ &= ac-bd+3(ad+bc)+5\mathbb{Z}\\ &= \phi(ac-bd+(ad+bc)i)\\ &= \phi((a+bi)\cdot(c+di)).\end{aligned}$$

- ϕ is surjective: $\phi(1) = 1+5\mathbb{Z}$ so $\phi(n) = n+5\mathbb{Z}$.

- $\ker\phi = \langle 2+i\rangle$: $\phi(2+i) = 2+3+5\mathbb{Z} = 0+5\mathbb{Z}$. So $\langle 2+i\rangle \subset \ker\phi$. Let $a \in \ker\phi$. By the division algorithm in $\mathbb{Z}[i]$, $\exists q, r \in \mathbb{Z}[i]$ such that $a = q(2+i)+r$ with $N(r) < N(2+i) = 5$. Let $r = r_1 + r_2 i$ so $N(r) = r_1^2 + r_2^2 < 5$. This implies $|r_1| \le 2$ and $|r_2| \le 2$. Moreover, $\phi(r) = \phi(a) = 0$ implies $5 \mid r_1 + 3r_2$. If $|r_1| = 2$, then $r_1^2 + r_2^2 < 5$ forces $r_2 = 0$ and so $r_1 + 3r_2 = r_1 = \pm 2$ is not divisible by 5; if $|r_2| = 2$, then $r_1 = 0$ and $r_1 + 3r_2 = 3r_2 = \pm 6$ is not divisible by 5. So $|r_1| \le 1$ and $|r_2| \le 1$.

  Remark. *Recall in the process of proving $\mathbb{Z}[i]$ is a Euclidean domain, not only do we show that $N(r) < N(\beta)$, we show $N(r) \le \frac{1}{2}N(\beta)$, where β is the divisor and r is the remainder. With this stronger bound on $N(r)$, we immediately have $r_1^2 + r_2^2 \le \frac{5}{2}$ and $|r_1| \le 1$ and $|r_2| \le 1$.*

  Then $|r_1 + 3r_2| < 5$. Together with $5 \mid r_1 + 3r_2$, this implies $r_1 + 3r_2 = 0$ and $3 \mid r_1$. However, $|r_1| \le 1$. So $r_1 = r_2 = 0$. So, $a \in \langle 2+i\rangle$ and $\ker\phi \subset \langle 2+i\rangle$.

Hence the conclusion follows by the first isomorphism theorem. ■

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

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

Proof. Let $\varphi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ be given by $x \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$.

- φ is a ring homomorphism:

  $$\begin{aligned}\varphi(x) + \varphi(y) &= (x + m\mathbb{Z}, x + n\mathbb{Z}) + (y + m\mathbb{Z}, y + n\mathbb{Z}) \\ &= ((x+y) + m\mathbb{Z}, (x+y) + n\mathbb{Z}) \\ &= \varphi(x+y)\end{aligned}$$

  and

  $$\begin{aligned}\varphi(x) \cdot \varphi(y) &= (x + m\mathbb{Z}, x + n\mathbb{Z}) \cdot (y + m\mathbb{Z}, y + n\mathbb{Z}) \\ &= (xy + m\mathbb{Z}, xy + n\mathbb{Z}) \\ &= \varphi(xy).\end{aligned}$$

- $$\ker\varphi = \{x \in \mathbb{Z} : x + m\mathbb{Z} = 0 + m\mathbb{Z}, x + n\mathbb{Z} = 0 + n\mathbb{Z}\} = \{x \in \mathbb{Z} : m \mid x, n \mid x\}.$$

  Since $(m,n) = 1$, $m \mid x, n \mid x \iff mn \mid x \iff x \in mn\mathbb{Z}$. Hence, $\ker\varphi = mn\mathbb{Z}$.

By the first isomorphism theorem, $\overline{\varphi} : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, x + mn\mathbb{Z} \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$ is an injection and an isomorphism onto $\mathrm{Im}\varphi$. Observe that $|\mathbb{Z}/mn\mathbb{Z}| = mn$ and $|\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = |\mathbb{Z}/m\mathbb{Z}| \cdot |\mathbb{Z}/n\mathbb{Z}| = mn$. By the pigeonhole principle, $\mathrm{Im}\varphi = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and hence $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. ■

4. Prove that $\mathbb{Z}[x]/n\mathbb{Z}[x] \simeq (\mathbb{Z}/n\mathbb{Z})[x]$.

Proof. Let $\varphi : \mathbb{Z}[x] \to (\mathbb{Z}/n\mathbb{Z})[x]$ be given by $\sum_{i=0}^m a_i x^i \mapsto \sum_{i=0}^m (a_i + n\mathbb{Z})x^i$. φ is clearly surjective and

$$\ker\varphi = \{\sum_{i=0}^m a_i x^i \in \mathbb{Z}[x] : a_i \in n\mathbb{Z}, i = 0, \cdots, m\} = n\mathbb{Z}[x].$$

Thus the conclusion follows by the first isomorphism theorem. ■

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

Proof. Let $\phi : \mathbb{Q}[x] \to M_2(\mathbb{Q})$ be the evaluation ring homomophism at A, i.e. $\phi(\sum_{i=0}^n a_i x^i) = a_0 I + a_1 A + \cdots + a_n A^n$. Let $C = \{c_0 I + c_1 A | c_0, c_1 \in \mathbb{Q}\}$.

Remark. *Note that the characteristic polynomial is $f_A(x) = \det(xI - A) = x^2 - 2x + 6$. Cayley-Hamilton theorem says that every square matrix over a commutative ring satisfies its own characteristic polynomial. So, $A^2 - 2A + 6 = 0$. If you've never heard of this theorem, you do now. For this problem, show $A^2 - 2A + 6 = 0$ by direct computation.*

- $\mathrm{Im}\phi = C$: for every $c_0, c_1 \in \mathbb{Q}$, $\phi(c_0 + c_1 x) = c_0 I + c_1 A$ so $C \subset \mathrm{Im}\phi$. Conversely, let $g(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Q}[x]$ so that $\phi(g) = \sum_{i=0}^n a_i A^i$. By the remark above, $A^2 = 2A - 6$. So, $A^i = A^{i-2}(2A - 6) = 2A^{i-1} - 6A^{i-2}$ for $i \geq 2$. This shows we can reduce any power of A to linear term. By induction, $\phi(g) \in C$ and $\mathrm{Im}\phi \subset C$.
- $\ker\phi = \langle x^2 - 2x + 6\rangle$: $A^2 - 2A + 6 = 0$ implies $\langle x^2 - 2x + 6\rangle \subset \ker\phi$. Let $h(x) \in \ker\phi$. By the division algorithm in $\mathbb{Q}[x]$, $\exists q(x), r(x) \in \mathbb{Q}[x]$ such that $h(x) = q(x)(x^2 - 2x + 6) + r(x)$, where $\deg r < 2$. Let $r(x) = c_1 x + c_0$. Then $\phi(r) = \phi(h) = 0$ implies $c_1 A + c_0 = 0$. So, $c_0 = c_1 = 0$ and $h(x) \in \langle x^2 - 2x + 6\rangle$. Hence, $\ker\phi \subset \langle x^2 - 2x + 6\rangle$.

The conclusion follows by the first isomorphism theorem.

■