

Math 5286H

Midterm 1 Solutions

Note that the writeup here is somewhat terse. If you have difficulty reconstructing the proof from what you see here please ask.

1. (a) Describe all possible ring homomorphisms $\mathbb{Z}[x]/(x^2 + 1) \rightarrow \mathbb{Z}/8$.

Solution. By the universal properties for polynomial algebras and quotient rings, a ring homomorphism ϕ from this ring to $\mathbb{Z}/8$ is equivalent to a choice of element $\phi(x)$ satisfying $\phi(x)^2 + 1 = 0$. However, there are no elements of $\mathbb{Z}/8$ satisfying this equation, and so there are no such ring homomorphisms.

- (b) Describe all possible ring homomorphisms $\mathbb{Z}[x]/(x^5 - x) \rightarrow \mathbb{Z}/5$.

Solution. As above, by the universal property this is the same as a choice of element $\phi(x) \in \mathbb{Z}/5$ satisfying $\phi(x)^5 = \phi(x)$. However, *all five* elements of $\mathbb{Z}/5$ satisfy this relation (that's Fermat's little theorem), and so there are 5 different ring homomorphisms, each sending x to a different element of $\mathbb{Z}/5$.

2. (a) Show that the element $\sqrt{2} + 1$ is a unit in the ring $\mathbb{Z}[\sqrt{2}]$.

Solution. In this ring, $(\sqrt{2} + 1)(\sqrt{2} - 1) = 1$, so this element is a unit.

- (b) Prove that the ring $\mathbb{Z}[\sqrt{2}]$ has infinitely many units.

Solution. For any nonnegative integer n , we have $(\sqrt{2} + 1)^n$ is a unit with inverse $(\sqrt{2} - 1)^n$. These are all distinct, because $\mathbb{Z}[\sqrt{2}]$ is a subring of \mathbb{R} and the elements $(\sqrt{2} + 1)^n$ are strictly increasing as n increases.

- (c) Show that the Gaussian integers $\mathbb{Z}[i]$ have only finitely many units.

Solution. If $a + bi$ is a unit with inverse $c + di$, then we have $1 = (a + bi)(c + di)$. Multiplying by $(a - bi)(c - di)$, we find

$$1 = (a^2 + b^2)(c^2 + d^2)$$

and so, because $a^2 + b^2$ and $c^2 + d^2$ are both positive integers, we must have $1 = a^2 + b^2$. The only possibilities are $a = \pm 1, b = 0$ or $a = 0, b = \pm 1$. Therefore, the only units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.

3. Let $a, b, c, d \in \mathbb{Z}$. Prove that the ring $\mathbb{Z}[x, y]/(ax + by, cx + dy)$ is isomorphic to \mathbb{Z} if and only if the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ has determinant ± 1 .

Solution. First, note: this matrix A has determinant ± 1 if and only if it has an inverse with integer entries. So we will show this matrix has an integer inverse if and only if the quotient ring is isomorphic to \mathbb{Z} .

Second, note: we have a containment of ideals $(cx + dy, ax + by) \subset (x, y)$.

First implication. If A has an integer inverse B , then we find the following equalities of matrix products.

$$\begin{bmatrix} x \\ y \end{bmatrix} = BA \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a'(ax + by) + b'(cx + dy) \\ c'(ax + by) + d'(cx + dy) \end{bmatrix}$$

Then

$$x = a'(ax + by) + b'(cx + dy) \in (ax + by, cx + dy)$$

and similarly

$$y = c'(ax + by) + d'(cx + dy) \in (ax + by, cx + dy)$$

and so we would have a containment of ideals $(x, y) \subset (ax + by, cx + dy)$. Therefore, $(x, y) = (ax + by, cx + dy)$ by the second note above. Thus, our ring is

$$\mathbb{Z}[x, y]/(ax + by, cx + dy) = \mathbb{Z}[x, y]/(x, y) \cong \mathbb{Z}.$$

Reverse implication. Suppose that the quotient ring $\mathbb{Z}[x, y]/(ax + by, cx + dy)$ is isomorphic to \mathbb{Z} . By the second note above, because $(x, y) \supset (ax + by, cx + dy)$, the correspondence theorem tells us that the quotient ring contains an ideal $(x, y)/(ax + by, cx + dy)$. Note that this ideal in the quotient ring does not contain any nonzero elements $n \in \mathbb{Z}$, because the correspondence theorem would then tell us that in the ring $\mathbb{Z}[x, y]$, we would have $(x, y) \supset (ax + by, cx + dy, n)$, which is false; n is not in the ideal (x, y) .

Since the quotient ring is supposed to be isomorphic to \mathbb{Z} , this means that the quotient ideal $(x, y)/(ax + by, cx + dy)$ can only be carried by this isomorphism to the unique ideal of \mathbb{Z} that does not contain any nonzero integers: the zero ideal. But then the two ideals $(ax + by, cx + dy)$ and (x, y) both correspond to the zero ideal, and hence the correspondence theorem tells us that they must be equal.

Therefore, this means that $x = f(x, y)(ax + by) + g(x, y)(cx + dy)$ and $y = h(x, y)(ax + by) + k(x, y)(cx + dy)$ for some elements f, g, h, k in the ring. Expanding out and looking at the linear terms, we find that the matrix

$$\begin{bmatrix} f(0, 0) & g(0, 0) \\ h(0, 0) & k(0, 0) \end{bmatrix}$$

is an inverse of A with integer entries.

4. Find all prime ideals in the ring $\mathbb{Z}[x]/(x^3 - 1)$ that contain the element 3.

Solution. If \mathfrak{P} is a prime ideal of this ring that contains 3, then

$$(x - 1)^3 = (x^3 - 1) - 3x^2 + 3x = 3(x - x^2) \in \mathfrak{P}.$$

Because \mathfrak{P} is prime, whenever a product of elements is in \mathfrak{P} one of the factors must be. However, this implies that $(x - 1)$ must be in \mathfrak{P} . Therefore, $\mathfrak{P} \supset (3, x - 1)$.

However, I claim that the ideal $(3, x - 1)$ is already maximal, which would force $\mathfrak{P} = (3, x - 1)$. To show that it is a maximal ideal, we only need to show that the quotient ring is a field. By applying the third isomorphism theorem a few times, we find

$$\begin{aligned} \frac{\mathbb{Z}[x]/(x^3 - 1)}{(3, x - 1)} &\cong \mathbb{Z}[x]/(3, x - 1, x^3 - 1) \\ &\cong \mathbb{Z}/3[x]/(x - 1, x^3 - 1) \\ &\cong \mathbb{Z}/3. \end{aligned}$$

This is a field, and so $(3, x - 1)$ is the unique prime ideal containing 3.

5. Suppose R is an integral domain.

- (a) Prove that if $r \in R$ is a root of a polynomial $f(x) \in R[x]$, and $f(x) = g(x)h(x)$, then r is either a root of g or h .

Solution. If $f(r) = 0$, then $g(r)h(r) = 0$, and since R is an integral domain we have $g(r) = 0$ or $h(r) = 0$.

- (b) Prove that a degree n monic polynomial $f(x) \in R[x]$ has at most n distinct roots.

Solution. We prove this by induction. If $f(x)$ is a constant monic polynomial, $f(x) \equiv 1$ which has no roots.

Now assume $f(x)$ is monic of degree n , and α is a root. Then $f(x) = (x - \alpha)g(x)$ for a monic polynomial $g(x)$ of degree $n - 1$. Then an element β is a root of $f(x)$ if and only if it is a root of $(x - \alpha)$ (which is only true if $\beta = \alpha$) or a root of $g(x)$. By the inductive hypothesis $g(x)$ has at most $n - 1$ distinct roots, and so $f(x)$ has at most n distinct roots: α and the roots of $g(x)$.