Algebraic Structures II, MAT 574, Homework 7

Part I

Chapter 14

20. Let $I = (2)$. Prove that $I[x]$ is not a maximal ideal of $\mathbb{Z}[x]$ even though I is a maximal ideal of $\mathbb{Z}$.

Proof. The ideal $I = (2)$ is a maximal ideal of $\mathbb{Z}$ because $\mathbb{Z}/I = \{I,\ 1+I\}$ is a field.

Notice that $I[x] = \{g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in (2) = I,\ \ n \text{ positive integer}\}$. Let $L = (x, 2) = \{f(x) \in \mathbb{Z}[x] \mid f(0) \text{ is an even integer}\}$. Then L is a proper ideal of $\mathbb{Z}[x]$ (Problem 35). For every $g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in I[x]$, we have $g(0) = a_0 \in (2)$ so that $g(x) \in L$. This proves that L contains $I[x]$. But $L \neq I[x]$. For example, $x + 2 \in L$ but $x + 2 \notin I[x]$. Thus L contains $I[x]$ properly, that is, $I[x]$ is not a maximal ideal. □

29. Let R be the ring of continuous functions from $\mathbb{R}$ to $\mathbb{R}$. Show that

$$A = \{f \in R \mid f(0) = 0\}$$

is a maximal ideal of R.

Proof. First we show that A is an ideal of R. Let $f(x)$ and $g(x)$ be elements of A. Then we obtain $(f-g)(0) = f(0) - g(0) = 0 - 0 = 0$ so that $f - g \in A$. Also for $h(x) \in R$ and $f(x) \in A$, we get $(h \cdot f)(0) = h(0) \cdot f(0) = h(0) \cdot 0 = 0$ so that $h \cdot f \in A$.

Now we show that R/A is a field. It is enough to show that for every nonzero element $h(x) + A \neq A$ of R/A, there exists the multiplicative inverse of $h(x) + A$. Since $h(x) \notin A$, we have $h(0) \neq 0$ in the field $\mathbb{R}$. Therefore there exists $c = \dfrac{1}{h(0)} \in \mathbb{R}$. Now let $w(x) = c$ be the constant function so that $w \in R$. Consider $v(x) = h(x)w(x) - 1 \in R$, where 1 is the constant function. Then

$$v(0) = h(0)w(0) - 1 = h(0)c - 1 = h(0)\frac{1}{h(0)} - 1 = 0,$$

which shows that $v(x) \in A$. In particular $h(x)w(x) - 1 \in A$ or $h(x)w(x) + I = 1 + I$. Therefore we get

$$(h(x) + I)(w(x) + I) = 1 + I,$$

which means that $w(x) + I$ is the multiplicative inverse of $h(x) + I$. □

35. In $\mathbb{Z}[x]$, let $I = \{f(x) \in \mathbb{Z}[x] \mid f(0) \text{ is an even integer}\}$.

(a) Prove that $I = (x, 2)$.

(b) How many elements does $\mathbb{Z}[x]/I$ have?

(c) Is I a maximal ideal of $\mathbb{Z}[x]$?

(d) Is I a prime ideal of $\mathbb{Z}[x]$?

Proof.

(a) Let $F(x) \in (x, 2)$. Then $F(x) = xg(x) + 2h(x)$ for some $g(x), h(x) \in \mathbb{Z}[x]$. Let $g(x) = \sum_{i=0}^{n} a_i x^i$ and $h(x) = \sum_{j=0}^{m} b_j x^j$. Then

$$F(x) = x \sum_{i=0}^{n} a_i x^i + 2 \sum_{j=0}^{m} b_j x^j = x \left(\sum_{i=0}^{n} a_i x^i + \sum_{j=1}^{m} 2b_j x^{j-1} \right) + 2b_0.$$

Therefore we may assume that $(x, 2) = \{xg(x) + 2c \mid g(x) \in \mathbb{Z}[x],\ \ c \in \mathbb{Z}\}$.

Let $f(x) = \sum_{i=0}^{l} d_i x^i \in I$. Then $f(0) = d_0 = 2s$ for some $s \in \mathbb{Z}$. Hence

$$f(x) = x \left(\sum_{j=1}^{l} d_j x^{j-1} \right) + d_0 = x \left(\sum_{j=1}^{l} d_j x^{j-1} \right) + 2s \in (x, 2).$$

Let $F(x) \in (x, 2)$. Then $F(x) = xg(x) + 2c$ for some $g(x) \in \mathbb{Z}[x]$ and $c \in \mathbb{Z}$. Then $F(0) = 0 \cdot g(0) + 2c = 2c$ so that $F(x) \in I$.

(b) Let $f(x) + I \in \mathbb{Z}[x]/I$. If $f(x) \notin I$, then $f(0)$ is odd. Hence $f(x)$ is of the form

$$f(x) = xg(x) + 2c + 1$$

for some $g(x) \in \mathbb{Z}[x]$. Then $f(x) - 1 = xg(x) + 2c \in I$ so that $f(x) + I = 1 + I$. Therefore $\mathbb{Z}[x]/I$ has two elements, I and $1 + I$.

(c) (d) Since $\mathbb{Z}[x]/I = \{I,\ 1 + I\}$ is a field, the ideal I is a maximal ideal. Therefore it is a prime ideal as well. □

55. Let R be a commutative ring with unity that has the property that $a^2 = a$ for all $a \in R$. Let I be a prime ideal of R. Show that $\mid R/I \mid = 2$.

Proof. Let $a + I \in R/I$. Suppose $a \notin I$. By assumption $a^2 = a$, or $a(a-1) = 0 \in I$. Since I is a prime ideal and $a \notin I$, we have $a - 1 \in I$. This means that $a + I = 1 + I$. Therefore $R/I = \{I,\ 1 + I\}$. $\square$

Chapter 15

10. Let $\mathbb{Z}_3[i] = \{a + b\,i \mid a, b \in \mathbb{Z}_3\}$. Show that the field $\mathbb{Z}_3[i]$ is ring-isomorphic to the field $\mathbb{Z}_3[x]/(x^2+1)$.

Proof. Let $I = (x^2 + 1)$ be an ideal of $\mathbb{Z}_3[x]$. Define $\phi : \mathbb{Z}_3[i] \longrightarrow \mathbb{Z}_3[x]/I$ to be

$$\phi(a + b\,i) = a + b\,x + I.$$

Let $a + b\,i$ and $c + di$ be elements of $\mathbb{Z}_3[i]$. Then

$$\begin{aligned}
\phi(a + b\,i + c + di) = \phi((a+c) + (b+d)i) &= (a+c) + (b+d)x + I \\
&= (a + b\,x + I) + (c + dx + I) \\
&= \phi(a + b\,i) + \phi(c + di).
\end{aligned}$$

$$\phi((a + b\,i)(c + di)) = \phi((ac - bd) + (ad + bc)i) = (ac - bd) + (ad + bc)x + I.$$

Notice that since $x^2 + 1 \in I$, we have $x^2 + I = -1 + I$. Therefore

$$\begin{aligned}
\phi(a + b\,i)\phi(c + di) = (a + bx + I)(c + dx + I) &= (a + bx)(c + dx) + I \\
&= ac + (ad + bc)x + bdx^2 + I \\
&= (ac + (ad + bc)x + I) + (bd + I)(x^2 + I) \\
&= (ac + (ad + bc)x + I) + (bd + I)(-1 + I) \\
&= (ac + (ad + bc)x + I) + (-bd + I) \\
&= (ac - bd) + (ad + bc)x + I.
\end{aligned}$$

In order to show that ϕ is one-to-one, suppose $\phi(a+b\,i)=\phi(c+di)$. Then

$$\begin{aligned} & a+bx+I=c+dx+I \\ \Longrightarrow\quad & a-c+(b-d)x\in I. \\ \Longrightarrow\quad & a-c+(b-d)x=(x^2+1)g(x) \quad \text{for some } \; g(x)\in\mathbb{Z}_3[x]. \end{aligned}$$

By comparing the degrees of both sides of this equation, we have $a-c+(b-d)x=0$ or $a=c$ and $b=d$.

For every element $a+b\,x+I\in\mathbb{Z}_3[x]/I$, there exists $a+b\,i\in\mathbb{Z}_3[i]$ such that $\phi(a+b\,i)=a+b\,x+I$. Hence ϕ is onto. □

12. Let $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$. Let

$$H=\left\{\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \mid a,b\in\mathbb{Z}\right\}.$$

Show that $\mathbb{Z}[\sqrt{2}]$ and H are isomorphic as rings.

Proof. Define $\phi:\mathbb{Z}[\sqrt{2}]\to H$ to be $\phi(a+b\sqrt{2})=\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$. Let $a+b\sqrt{2}$ and $c+d\sqrt{2}$ be elements of $\mathbb{Z}[\sqrt{2}]$. Then

$$\begin{aligned} \phi(a+b\sqrt{2}+c+d\sqrt{2}) &= \phi((a+c)+(b+d)\sqrt{2}) \\ &= \begin{bmatrix} a+c & 2(b+d) \\ b+d & a+c \end{bmatrix} \\ &= \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}+\begin{bmatrix} c & 2d \\ d & c \end{bmatrix} \\ &= \phi(a+b\sqrt{2})+\phi(c+d\sqrt{2}). \end{aligned}$$

$$\begin{aligned}
\phi((a+b\sqrt{2})(c+d\sqrt{2})) &= \phi((ac+2bd)+(ad+bc)\sqrt{2}) \\
&= \begin{bmatrix} ac+2bd & 2(ad+bc) \\ ad+bc & ac+2bd \end{bmatrix} \\
&= \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}\begin{bmatrix} c & 2d \\ d & c \end{bmatrix} \\
&= \phi(a+b\sqrt{2})\phi(c+d\sqrt{2}).
\end{aligned}$$

Suppose $\phi(a+b\sqrt{2}) = \phi(c+d\sqrt{2})$. Then $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} = \begin{bmatrix} c & 2d \\ d & c \end{bmatrix}$ so that $a = c$ and $b = d$. This proves that ϕ is one-to-one.

For every element $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \in H$, there exists $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ such that $\phi(a+b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$. This shows that ϕ is onto. □

13. Consider the mapping ϕ from $M_2(\mathbb{Z})$ into $\mathbb{Z}$ given by $\begin{bmatrix} a & b \\ c & c \end{bmatrix} \longrightarrow a$. Prove or disprove that this is a ring homomorphism.

Proof. This is not a ring homomorphism because the multiplication is not preserved under the map. For example, let $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix}$. Then we have

$$\phi(AB) = \phi\left(\begin{bmatrix} 5 & 11 \\ 11 & 25 \end{bmatrix}\right) = 5 \quad \text{but} \quad \phi(A)\phi(B) = 1 \cdot 1 = 1.$$

□

Part II

Notation 1 Let R be a ring and I an ideal of R.

(a) $R \setminus I = \{r \in R \mid r \notin I\}$.

(b) $\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some positive integer } n\}$.

1. Let R be a commutative ring with unity 1 and M a proper ideal of R. Prove that M is a maximal ideal of R if and only if for every element $r \in R \setminus M$, there exists $x \in R$ such that $1 - rx \in M$.

Proof. Suppose M is a maximal ideal. Let $r \in R \setminus M$. Consider the ideal $N = M + (r)$. Then since $r \notin M$, we have $M \subsetneq N$. Then since M is a maximal ideal, $N = R$. In particular $1 \in N = M + (r)$. Therefore there exist $m \in M$ and $x \in R$ such that $1 = m + rx$. Hence $1 - rx = m \in M$.

Assume that for every element $r \in R \setminus M$, there exists $x \in R$ such that $1 - rx \in M$. Suppose that there exists an ideal L of R such that $M \subseteq L \subseteq R$. Suppose that $M \neq L$. Then there exists $r \in L \setminus M$. By assumption, there exists $x \in R$ such that $1 - rx \in M$. This means that $1 - rx = m$ for some element $m \in M$. Therefore $1 = rx + M \in L$, that is, $R = L$. □

2. Let R be a commutative ring with unity. Let Q be a proper ideal of R such that whenever $ab \in Q$ but $a \notin Q$, there exists a positive integer m such that $b^m \in Q$. Prove that $\sqrt{Q}$ is a prime ideal.

Proof. Suppose $xy \in \sqrt{Q}$ and $x \notin \sqrt{Q}$. Then $(xy)^n = x^n y^n \in Q$ for some positive integer n. Since $x^n \notin \sqrt{Q}$, by the assumption, $(y^n)^m \in Q$ for some positive integer m. Therefore $y^{nm} \in Q$ so that $y \in \sqrt{Q}$. □

3. Let R be a commutative ring and I an ideal of R. Prove that every ideal of R/I can be expressed as $J/I = \{a + I \mid a \in J\}$, where J is an ideal of R containing I.

Proof. First we show that $K/I = \{a + I \mid a \in K\}$ is an ideal of R/I for any ideal K of R containing I. Let $a + I$ and $b + I$ be elements of K/I with $a, b \in K$. Then $a - b \in K$ since K is an ideal. Therefore

$$(a + I) - (b + I) = (a - b) + I \in K/I.$$

For $r + I \in R/I$ and $a + I \in K/I$, we have $ra \in K$ since K is an ideal. Therefore

$$(r + I)(a + I) = ra + I \in K/I.$$

This proves that K/I is an ideal of R/I.

Let L be an ideal of R/I and let $J = \{r \in R \mid r + I \in L\}$. Then J is an ideal of R. Indeed, if $a, b \in J$, then $a + I \in L$ and $b + I \in L$. Since L is an ideal, we have

$$(a - b) + I = (a + I) - (b + I) \in L,$$

which shows that $a - b \in J$. Also if $x \in R$ and $a \in J$, then $x + I \in R/I$ and $a + I \in L$. Since L is an ideal, we obtain

$$(xa) + I = (x + I)(a + I) \in L,$$

which proves that $xa \in J$.

Moreover J contains I because for every element $c \in I$, we have $c + I = I \in L$ (Note that I is the additive identity element in R/I and every ideal of R/I contains the additive identity element).

Now it is enough to show that $L = J/I$, where $J = \{r \in R \mid r + I \in L\}$. For every element $x + I \in L$, by the definition of J, we get $x \in J$ so that $x + I \in J/I$. Also for every element $y + I \in J/I$, since $x \in J$, by the definition of J, we get $x + I \in L$. Therefore $L = J/I$. $\square$