Math 235 (Fall 2012)
Assignment 4 solutions

Luiz Kazuo Takei

November 17, 2012

Exercise 1

Yes, the set S is a subring of $M_2(R)$. Let us check this fact.

- $1_{M_2(R)} \in S$: in fact, $1_{M_2(R)} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in S$.
- S is closed under addition: let $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right), \left(\begin{smallmatrix} r & s \\ 0 & t \end{smallmatrix}\right) \in S$, then

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} r & s \\ 0 & t \end{pmatrix} = \begin{pmatrix} a+r & b+s \\ 0 & c+t \end{pmatrix} \in S.$$

- S is closed under multiplication: let $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right), \left(\begin{smallmatrix} r & s \\ 0 & t \end{smallmatrix}\right) \in S$, then

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} r & s \\ 0 & t \end{pmatrix} = \begin{pmatrix} ar & as+bt \\ 0 & ct \end{pmatrix} \in S.$$

Exercise 2

Let R be a subring of $\mathbb{Q}$. Then $1 \in R$. Since R is closed under addition,

$$2 = 1+1 \ , \ 3 = 2+1 \ , \ 4 = 3+1 \ , \ \ldots \ \in R.$$

By induction, it is easy to see that $\mathbb{N} \subseteq R$. Therefore R can't be finite.

Exercise 3

Let $f : \mathbb{Q}(\sqrt{-2}) \to \mathbb{Q}(\sqrt{-2})$ be the given function, i.e.,

$$f(a + b\sqrt{-2}) = a - b\sqrt{-2}.$$

It is obvious that f is bijective. So it is enough to show that f is a homomorphism of rings.

First, let us show it preserves addition:

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

Now we check it preserves multiplication:

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

This finishes the exercise.

Exercise 4

[EXISTENCE]

Notice that $f:\mathbb{Z}\to R$ defined by

$$f(n) = \begin{cases} n\cdot 1_R := 1_R+\cdots+1_R, & n\geq 0 \\ -(|n|\cdot 1_R) := -(1_R+\cdots+1_R), & n<0 \end{cases}$$

(where $1_R+\cdots+1_R$ is the sum of 1_R taken n times) is a ring homomorphism.

[UNIQUENESS]

Now we show that f is the only possible homomorphism from $\mathbb{Z}$ to R. Let $g:\mathbb{Z}\to R$ be a homomorphism (possibly different from f). We want to show that g is necessarily equal to f.

By the axioms of a homomorphism, we have that $g(1)=1_R$. Using that g has to preserve addition, we obtain that $g(2)=g(1+1)=g(1)+g(1)=1_R+1_R=2\cdot 1_R$. Similarly, $g(3)=g(2+1)=g(2)+g(1)=3\cdot 1_R$. Using this idea, it is easy to show by induction that $g(n)=n\cdot 1_R$ for $n\geq 1$.

We know that for any homomorphism of rings $g(0)=0$ and $g(-n)=-g(n)$.

This shows that $g=f$, showing uniqueness.

Exercise 5

Let R be a finite integral domain. To show that R is a field, it is enough to show that any element $r\in R\backslash\{0\}$ has a multiplicative inverse.

So let $r\in R\backslash\{0\}$. Consider the set $\{r^n \mid n\geq 1\}\subseteq R$. Since R is finite, this set must also be finite. This means that there are $n,a>0$ such that $r^n=r^{n+a}$. This implies that

$$r^n(r^a-1)=0.$$

Since R has no zero divisors,

$$\text{either}\quad [r^n=0]\quad\text{or}\quad [r^a-1=0].$$

If $r^n=0$, since R has no zero divisors, $r=0$, which is a contradiction. Therefore, $r^a=1$. But this implies that

$$r\cdot r^{a-1}=1,$$

which shows that r^{a-1} is a multiplicative inverse of r.

Exercise 6

The subset $I = F \subset F[X] = R$ is not an ideal of R because $X \in R$, $1 \in F$ but $X = X \cdot 1 \notin I$.

Exercise 7

The subset I here is an ideal of $\mathbb{Z} \times \mathbb{Z}$. Let us check that

- I is closed under addition: if $(m,0),(n,0) \in I$, then

$$(m,0) + (n,0) = (m+n,0) \in I.$$

- I is closed under multiplication by an element of $\mathbb{Z} \times \mathbb{Z}$: if $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ and $(m,0) \in I$, then

$$(a,b) \cdot (m,0) = (am,0) \in I.$$

Exercise 8

Let N be the set of nilpotent elements of R (a commutative ring), i.e.,

$$N = \{s \in R \mid s^n = 0, \text{ for some } n > 0\}.$$

Then N is an ideal of R. Let us prove this fact:

- N is closed under multiplication by an element of R: if $r \in R$ and $s \in N$, then $s^n = 0$ for some $n > 0$ and, hence,

$$(rs)^n = r^n s^n = r^n \cdot 0 = 0,$$

which shows that $rs \in N$.

- N is closed under addition: if $s, t \in N$, then $s^a = t^b = 0$ for some $a, b > 0$ and, hence, by the binomial theorem,

$$(s+t)^{a+b} = \sum_{j=0}^{a+b} \binom{a+b}{j} s^j t^{a+b-j}.$$

Now, for each $j \in \{1, 2, \ldots, a+b\}$, we have that

$$\text{either} \quad [j \geq a] \quad \text{or} \quad [a+b-j \geq b],$$

which implies that

$$\text{either} \quad [s^j = 0] \quad \text{or} \quad [t^{a+b-j} = 0],$$

meaning that $(s+t)^{a+b} = 0$ and, thus, $s+t \in N$.

Now, if R is not commutative, then N is not necessarily an ideal of R. As an example, let $R = M_2(\mathbb{Z})$, which is not commutative, and $A = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \in R$. Then $A^2 = 0$, which implies that $A \in N$.

Now take $B = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \in R$. Then

$$C := B \cdot A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

is not in N (in fact, $C^n = C \neq 0$, for all $n > 0$).

Exercise 9

In this case, I is not an ideal. As a counter-example, take $f : \mathbb{Z} \to \mathbb{R}$ defined by $f(n) = 1$, for all $n \in \mathbb{Z}$. Clearly $f \in I$.

Now take $g : \mathbb{Z} \to \mathbb{R}$ defined by $g(n) = n$, which is an element of R.

Then gf is not an element of I. In fact,

$$(gf)(0) = g(0)f(0) = 0 \cdot 1 = 0 \neq 1 = g(1)f(1) = (gf)(1).$$

Exercise 10

In this case, I is an ideal. Let us prove this.

- I is closed under addition: if $f, g \in I$, then

  $$(f + g)(0) = f(0) + g(0) = 0 = f(1) + g(1) = (f + g)(1)$$

  and, hence, $f + g \in I$.

- I is closed under multiplication by an element of R: if $f, g \in I$, then

  $$(fg)(0) = f(0)g(0) = 0 = f(1)g(1) = (fg)(1)$$

  and, hence, $fg \in I$.

Exercise 11

Let I be an ideal of $F[x]$. If $I = \{0\}$, then $I = (0)$ and the proof is finished. Assume now that $I \neq \{0\}$.

Consider the set $X = \{n \in \mathbb{N} \mid \deg(f(x)) = n \text{ for some } f(x) \in I \backslash \{0\}\}$. The set $X \subseteq \mathbb{N}$ is clearly non-empty and, hence, by the well-ordering principle, there exists

$$n_0 = \min X$$

the smallest number in X.

By construction, there is a polynomial $f_0(x) \in I$ such that $\deg(f_0(x)) = n_0$ and any other polynomial of I has degree at least n_0. The exercise will be finished with the claim below.

Claim. The ideal I is generated by $f_0(x)$, i.e.,

$$I = (f_0(x)).$$

Proof. By the axioms of an ideal, it is easy to see that $(f_0(x)) \subseteq I$. Therefore, it suffices to show that $I \subseteq (f_0(x))$.

Take $f(x) \in I$. We know, by Euclidean division, that there exists polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)f_0(x) + r(x)$$

and $\deg(r(x)) < n_0$ or $r(x) = 0$.

But then $r(x) = f(x) - q(x)f_0(x) \in I$ (because both $f(x)$ and $f_0(x)$ are in I. By the minimality of n_0, it follows that $r(x) = 0$. Hence

$$f(x) = q(x)f_0(x) \in (f_0(x)).$$

□

We now prove that $\mathbb{Z}[x]$ has ideals that are not principal. Consider the ideal

$$J := (2, x) = \{2f(x) + xg(x) \mid f(x), g(x) \in \mathbb{Z}[x]\} \subseteq \mathbb{Z}[x].$$

Claim. The ideal J is not the whole ring $\mathbb{Z}[x]$.

Proof. If it was, we would have that $1 \in J$, i.e.,

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

for some $f(x), g(x) \in \mathbb{Z}[x]$.

Then

$$1 = 2f(0),$$

with $f(0) \in \mathbb{Z}$, which is impossible because $1/2 \notin \mathbb{Z}$. □

Claim. The ideal J is not principal.

Proof. Assume, by contradiction, that J is principal, say

$$J = (f_0(x))$$

for some polynomial $f_0(x) \in \mathbb{Z}[x]$.

In particular, we have that

$$2 = f_0(x)r(x)$$

for some $r(x) \in \mathbb{Z}[x]$. Looking at the degrees, we obtain that $\deg(f_0(x)) = \deg(r(x)) = 0$. So, $f_0(x) = a_0, r(x) = r_0 \in \mathbb{Z}$. Moreover, $2 = a_0r_0$ says that $a_0 = \pm 1$ or ± 2.

a_0 cannot be ± 1 because then $J = \mathbb{Z}[x]$ (why?).

So $f_0(x) = a_0 = \pm 2$.

But $x \in J$ implies that

$$x = f_0 s(x) = \pm 2s(x)$$

for some $s(x) \in \mathbb{Z}[x]$, which is also impossible (why?).

This shows that our initial assumption (that J is principal) is not correct. □

Exercise 12

Let us start proving that $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

Recall that

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$$

and

$$i^2 = -1.$$

There is a natural homomorphism

$$\begin{array}{rccc} \varphi: & \mathbb{R}[x] & \longrightarrow & \mathbb{C} \\ & f(x) & \longmapsto & f(i) \end{array}$$

It is easy to see that φ is surjective. Therefore, by the isomorphism theorem,

$$\mathbb{R}[x]/\ker(\varphi) \cong \mathbb{C}.$$

Now we just need to show that

$$\ker(\varphi) = (x^2+1).$$

In case you don't remember: $\ker(\varphi) = \{f(x) \in \mathbb{R}[x] \mid \varphi(f(x)) = 0\} = \{f(x) \in \mathbb{R}[x] \mid f(i) = 0\}$.

By the proof of last exercise, the only thing we need to show is that $p(x) = x^2+1$ is a polynomial of smallest degree in $\ker(\varphi)$. Notice first that $p(x) \in \ker(\varphi)$ (this is clear because $i^2 - 1 = 0$). Now, if we take a non-zero polynomial of degree < 2, then it can't be in $\ker(\varphi)$. This follows from the fact that $a + bi$ can only be zero if $a = b = 0$.

We now prove the second part of the exercise: that $\mathbb{C}[x]/(x^2+1) \cong \mathbb{C} \times \mathbb{C}$.

Consider the homomorphism

$$\begin{array}{rccc} \psi: & \mathbb{C}[x] & \longrightarrow & \mathbb{C} \times \mathbb{C} \\ & f(x) & \longmapsto & (f(i), f(-i)) \,. \end{array}$$

Claim. The homomorphism ψ is surjective.

Proof. Take $(a+bi, c+di) \in \mathbb{C} \times \mathbb{C}$. We want to show that there is $f(x) \in \mathbb{C}[x]$ such that $f(i) = a + bi$ and $f(-i) = c + di$.

The following polynomial satisfies the desired property and shows that *psi* is surjective:

$$f(x) = \frac{a+bi}{2i}(x+i) + \frac{c+di}{-2i}(x-i).$$

□

Now, by the isomorphism theorem,

$$\mathbb{C}[x]/\ker(\psi) \cong \mathbb{C} \times \mathbb{C}.$$

Like before, our final job is to show that $\ker(\psi) = (x^2+1)$. And, again, this is the same as showing that the polynomial $p(x) = x^2+1$ is a polynomial of smallest degree in $\ker(\psi)$. This final step is pretty much the same as the final step of the first part of the exercise, so we leave it for you! :)

Exercise 13

It is easy to see that $\mathbb{Q}(\sqrt{-5})$ is a ring and that $\mathbb{Z}[\sqrt{-5}]$ is a subring of $\mathbb{Q}(\sqrt{-5})$. It suffices than to show that $\mathbb{Q}(\sqrt{-5})$ is a field, which amounts to showing that every non-zero element of it has a multiplicative inverse.

So take $a + b\sqrt{-5} \in \mathbb{Q}(\sqrt{-5})\backslash\{0\}$, i.e., $a, b \in \mathbb{Q}$ are not both zero. We want to show it has an inverse in $\mathbb{Q}(\sqrt{-5})$.

Note that (magic!)

$$(a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2 =: r \in \mathbb{Q}\backslash\{0\}$$

and, thus,

$$(a + b\sqrt{-5})(a/r - b/r\sqrt{-5}) = 1,$$

showing that

$$(a/r - b/r\sqrt{-5}) \in \mathbb{Q}(\sqrt{-5})$$

is a multiplicative inverse of $a + b\sqrt{-5}$.

Exercise 14

You are really brave! Reading the solution to the second optional problem! So let's continue!

Actually that magical little trick from the last exercise comes from a function known as the "norm function". Here it is in all its glory:

$$\begin{array}{rccl} N: & \mathbb{Q}(\sqrt{-5}) & \longrightarrow & \mathbb{Q} \\ & a + bi & \longmapsto & (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2. \end{array}$$

You can show that N preserves multiplication, i.e.,

$$N(zw) = N(z)N(w)$$

for all $z, w \in \mathbb{Q}(\sqrt{-5})$.

Moreover, if we restrict the norm function to $\mathbb{Z}[\sqrt{-5}]$, the image lands in $\mathbb{Z}$, i.e.,

$$\begin{array}{rccl} N: & \mathbb{Z}[\sqrt{-5}] & \longrightarrow & \mathbb{Z} \\ & a + bi & \longmapsto & (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2. \end{array}$$

We want to show that the only invertible elements in $\mathbb{Z}[\sqrt{-5}]$ are $1, -1$. Let $z \in \mathbb{Z}[\sqrt{-5}]$ be an invertible element. Then there exists an element $w \in \mathbb{Z}[\sqrt{-5}]$ such that

$$vw = 1.$$

But then taking norms,

$$N(v)N(w) = N(vw) = N(1) = 1$$

Calling $v = a + bi$, we have the following equation in $\mathbb{Z}$

$$(a^2 + 5b^2)N(w) = 1.$$

Since the equation is in $\mathbb{Z}$ we have that

$$a^2 + 5b^2 = \pm 1.$$

Hence the only possible values of a and b are:

$$a = \pm 1 \quad \text{and} \quad b = 0.$$

Therefore

$$z = \pm 1$$

as we wanted.

Notice we proved that an element $z \in \mathbb{Z}[\sqrt{-5}]$ is invertible if and only if $N(z) = 1$.

Exercise 15

Let us show that $2 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible. Assume that

$$2 = zw$$

for some $z, w \in \mathbb{Z}[\sqrt{-5}]$.

Our goal is to show that either z or w is invertible (i.e., either $N(z) = 1$ or $N(w) = 1$).

Taking norms yield

$$4 = N(2) = N(z)N(w).$$

Since $N(a + b\sqrt{-5}) = a^2 + 5b^2$, we see that the only solutions are

$$N(z) = 4 \text{ and } N(w) = 1$$

or

$$N(z) = 1 \text{ and } N(w) = 4.$$

In any case, either z or w is invertible, as we wanted.

The proof that the other numbers are irreducible is similar and will be left for you.

Exercise 16

We have the simple remark

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

which shows that we don't have unique factorization in $\mathbb{Z}[\sqrt{-5}]$.

Exercise 17

Let us prove that $I := (2, 1+\sqrt{-5})$ is not principal.

Suppose, by contradiction, that $I = (z)$. Then

$$\begin{aligned} 2 &= zw \\ 1+\sqrt{-5} &= zv \end{aligned}$$

for some $w, v \in \mathbb{Z}[\sqrt{-5}]$.

Taking norms yield

$$\begin{aligned} 4 &= N(z)N(w) \\ 6 &= N(z)N(v). \end{aligned}$$

By recalling that

$$N(a + b\sqrt{-5}) = a^2 + 5b^2,$$

we see that we must have

$$N(z) = 1,$$

which implies that $z = \pm 1$ which is not true (prove that $-1 \notin I$).

The same kind of argument proves that the other two ideals are not principal.

Let us now prove that $(2, 1+\sqrt{-5})$ is not a product of non-trivial prime ideals (in the sense defined in exercise 18). A "non-trivial" ideal here means an ideal that is not the whole ring.

We start with a claim.

Claim 1. *The ideal* $(2, 1+\sqrt{-5})$ *is a maximal ideal.*

Proof. Let J be an ideal such that

$$(2, 1+\sqrt{-5}) \subsetneq J.$$

Our goal is to show that J is necessarily the whole ring, i.e., that $1 \in J$.

Let $\alpha = a + b\sqrt{-5} \in J \backslash (2, 1+\sqrt{-5})$, where $a, b \in \mathbb{Z}$. Then we can write

$$a = 2m + \epsilon_a \quad \text{and} \quad b = 2n + \epsilon_b,$$

for some $m, n \in \mathbb{Z}$ and $\epsilon_a, \epsilon_b \in \{0, 1\}$.

Since $2(m + n\sqrt{-5}) \in (2, 1+\sqrt{-5})$, we obtain that

$$\epsilon_a + \epsilon_b\sqrt{-5} = \alpha - 2(m + n\sqrt{-5}) \in J \backslash (2, 1+\sqrt{-5}),$$

i.e., one of the following elements are in J (and not in $(2, 1+\sqrt{-5})$):

$$1, \quad \sqrt{-5}, \quad 1+\sqrt{-5}.$$

In any of these cases, since $1+\sqrt{-5} \in J$, we have that $1 \in J$. $\square$

Note that the product of two ideals is never an ideal bigger than the original ones, i.e.,

$$IJ \subseteq I \quad \text{and} \quad IJ \subseteq J.$$

Hence, if $(2, 1+\sqrt{-5}) = IJ$, then

$$I = (2, 1+\sqrt{-5}) \quad \text{or} \quad I = \mathbb{Z}[\sqrt{-5}]$$

and the same applies for J:

$$J = (2, 1+\sqrt{-5}) \quad \text{or} \quad J = \mathbb{Z}[\sqrt{-5}].$$

Since I and J can't both be $(2, 1+\sqrt{-5})$ (because exercise 18 says that, in this case $IJ = (2) \neq (2, 1+\sqrt{-5})$), we must have that either I is trivial or J is trivial.

A similar argument shows that the other two ideals are not product of two non-trivial ideals.

Exercise 18

Let us show that $(2, 1+\sqrt{-5})^2 = (2)$. It is easy to see that $(2, 1+\sqrt{-5})^2$ is generated by

$$2^2, 2(1+\sqrt{-5}), (1+\sqrt{-5})^2 = -4 + 2\sqrt{-5}$$

Since they are all multiples of 2, we have that $(2, 1+\sqrt{-5})^2 \subseteq (2)$.

Now, note that

$$2 = -(1+\sqrt{-5})^2 + 2(1+\sqrt{-5})$$

which implies that $(2) \subseteq (2, 1+\sqrt{-5})^2$.

The same kind of argument shows the other two equalities.

References