Solutions of Assignment 4
Basic Algebra I

October 7, 2004

Solution of the problem 1. For S to be a subring of R, it is enough to verify that:

(i) S it is closed under addition and multiplication. For addition it is almost obvious that S is closed. And for the multiplication, just note that:

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} \star & \star \\ 0 & \star \end{pmatrix} \in S.$$

(ii) $0_R \in S$, which is clear: $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in S$.

(iii) If $X = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in S$, then $-X \in S$, which is again clear.
Therefore, we conclud that S is a subring of R.

Solution of the problem 2. The only non-almost clear thing to check is being closed under multiplication:

$$\begin{pmatrix} a & \star \\ 0 & a \end{pmatrix} \begin{pmatrix} a' & \star \\ 0 & a' \end{pmatrix} = \begin{pmatrix} aa' & \star \\ 0 & aa' \end{pmatrix} \in S.$$

Thus, S is a subring of R.

Solution of the problem 3. If S is a subring of $\mathbb{Q}$, then according to the definition given in class, $1 \in S$, so S contains all the elements

$$1, 2 = 1 + 1, 3 = 1 + 1 + 1, \cdots,$$

hence it is infinite.

Remark Even according to the definition given in Hungerford's book, which does not require a subring have the same identity element as the whole ring, a slightly modified version of the above holds:

Every non-trivial "subring" S of $\mathbb{Q}$ (i.e., $S \neq \{0\}$) is infinite.

For the proof, choose any non-zero element of S and repeat the above argument.

Solution of the problem 4. In notations:

$$S = \{(a,\ 0_A) :\ a \in A\}.$$

That S is a ring with the zero element $0_S = (0_A,\ 0_A)$ and the identity element $1_S = (1_A,\ 0_A)$ needs just very simple verifications, left to students. Now let's define the following map:

$$g:\ A \to S,\quad g(a) = (a,\ 0_A).$$

By the definition, g is an isomorphism of rings if:

(i) It is injective (or one-to-one);

(ii) It is surjective (or onto);

(iii) $g(a + a') = g(a) + g(a')$ and $g(aa') = g(a)g(a')$ for all $a,\ a' \in S$.

Let's see why (i),(ii) and (iii) are true.

(i) g is injective, because if $g(a) = g(a')$ then $(a,\ 0_A) = (a',\ 0_A)$, and therefore $a = a'$.

(ii) Trivial!

(iii) Quite routine:

$$g(a + a') = (a + a',\ 0_A) = (a,\ 0_A) + (a',\ 0_A) = g(a) + g(a'),$$

and

$$g(aa') = (aa',\ 0_A) = (a,\ 0_A)(a',\ 0_A) = g(a)g(a').$$

And finally, S is not a subring of R, because they don't have the same identity elements: $1_S = (1_A,\ 0_A) \neq (1_A,\ 1_A) = 1_R$.

Solution of the problem 5. Assume that $ax = ay$, where $x, y \in R$. Since we are in a ring, we can rewrite the equality as $a(x - y) = 0$, and now since a is not a zero divisor, we conclude that $x - y = 0$ or $x = y$.

Solution of the problem 6. First of all note that

$$R = \{a + b\sqrt{2}:\ a, b \in \mathbb{Q}\}$$

with the usual binary operations of real numbers is a ring (check this!). Now we consider the following function:

$$\phi:\ R \longrightarrow R,\quad \phi(a + b\sqrt{2}) = a - b\sqrt{2}.$$

(i) To see why ϕ is injective, suppose that $\phi(a + b\sqrt{2}) = \phi(c + d\sqrt{2})$. So $a - b\sqrt{2} = c - d\sqrt{2}$ or

$$(b - d)\sqrt{2} = a - c.$$

Now if $b - d \neq 0$, then we would deduce that

$$\sqrt{2} = \frac{a - c}{b - d} \in \mathbb{Q},$$

which is absurd. This shows that $b = d$, and therefore $a = c$, i.e, $a + b\sqrt{2} = c + d\sqrt{2}$.

(ii) To show that ϕ is surjective, just note that

$$\phi(a - b\sqrt{2}) = a + b\sqrt{2}\ !$$

(iii) And finally, to prove that ϕ respects addition and multiplication, write $\alpha = a + b\sqrt{2},\ \beta = c + d\sqrt{2}$ and notice that

$$\begin{aligned} \phi(\alpha+\beta) &= \phi\Big((a+c)+(b+d)\sqrt{2}\Big) \\ &= (a+c)-(b+d)\sqrt{2} \\ &= (a-b\sqrt{2})+(c-d\sqrt{2}) \\ &= \phi(\alpha)+\phi(\beta), \end{aligned}$$

and

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

Therefore ϕ is an isomorphism.

Solution of the problem 7. Recall that 1_R denotes the identity element of the ring R. If $f : \mathbb{Z} \to R$ wants to be a ring homomorphism, by the very definition, we must have $f(1) = 1_R$. Therefore

$$f(2) = f(1+1) = f(1) + f(1) = 1_R + 1_R.$$

Likewise, we must have

$$f(3) = f(2+1) = f(2) + f(1) = 1_R + 1_R + 1_R.$$

A very simple inductive argument will reveal that for any natural number n, we must have

$$f(n) = \underbrace{1_R + \cdots + 1_R}_{n \text{ times}}. \qquad (\star)$$

Once again, if f wants to be a ring homomorphism, by a theorem proved in class, we must have $f(0) = 0_R$ (here 0_R stands for the zero element of R) and

$$f(-n) = -f(n) = -(\underbrace{1_R + \cdots + 1_R}_{n \text{ times}}) \qquad (\star\star).$$

All these show that if f is a ring homomorphism from the ring of integers $\mathbb{Z}$ to an arbitrary ring R with the identity element 1_R, the crucial condition $f(1) = 1_R$ will determine f uniquely. In other words, if there exists a ring homomorphism from $\mathbb{Z}$ to R, then it has to be unique. The fact that if we actually define f by using $(\star)$ and $(\star\star)$, then it will be a ring homomorphism, is an easy exercise, left to the reader!

Solution of the problem 8. There are two non-trivial things to check:

(i) Multiplication in $R[i]$ is associative. To see this, write $\alpha_i = (a_i,\ b_i)$ for $i = 1, 2, 3$. From one hand we have

$$\begin{aligned}
(\alpha_1\alpha_2)\alpha_3 &= (a_1a_2 - b_1b_2,\ a_1b_2 + a_2b_1)(a_3,\ b_3) \\
&= ((a_1a_2 - b_1b_2)a_3 - (a_1b_2 + a_2b_1)b_3,\ (a_1a_2 - b_1b_2)b_3 + (a_1b_2 + a_2b_1)a_3) \\
&= (a_1a_2a_3 - b_1b_2a_3 - a_1b_2b_3 - a_2b_1b_3,\ a_1a_2b_3 - b_1b_2b_3 + a_1b_2a_3 + a_2b_1a_3).
\end{aligned}$$

And on the other hand

$$\begin{aligned}
\alpha_1(\alpha_2\alpha_3) &= (a_1,\ b_1)\,(a_2a_3 - b_2b_3,\ a_2b_3 + a_3b_2) \\
&= (a_1(a_2a_3 - b_2b_3) - b_1(a_2b_3 + a_3b_2),\ a_1(a_2b_3 + a_3b_2) + b_1(a_2a_3 - b_2b_3)) \\
&= (a_1a_2a_3 - b_1b_2a_3 - a_1b_2b_3 - a_2b_1b_3,\ a_1a_2b_3 - b_1b_2b_3 + a_1b_2a_3 + a_2b_1a_3).
\end{aligned}$$

Therefore, $(\alpha_1\alpha_2)\alpha_3 = \alpha_1(\alpha_2\alpha_3)$.

(ii) Distribution law holds. To show this, note that on one hand

$$\begin{aligned}
\alpha_1(\alpha_2 + \alpha_3) &= (a_1,\ b_1)(a_2 + a_3,\ b_2 + b_3) \\
&= (a_1(a_2 + a_3) - b_1(b_2 + b_3),\ a_1(b_2 + b_3) + b_1(a_2 + a_3)) \\
&= (a_1a_2 + a_1a_3 - b_1b_2 - b_1b_3,\ a_1b_2 + a_1b_3 + b_1a_2 + b_1a_3)
\end{aligned}$$

On the other hand one can also check that

$$\alpha_1\alpha_2 + \alpha_1\alpha_3 = (a_1a_2 + a_1a_3 - b_1b_2 - b_1b_3,\ a_1b_2 + a_1b_3 + b_1a_2 + b_1a_3).$$

Thus $\alpha_1(\alpha_2 + \alpha_3) = \alpha_1\alpha_2 + \alpha_1\alpha_3$ and we are done.

Solution of the problem 9. To prove that

$$S = \{(r,\ o) :\ r \in R\}$$

is a subring of $R[i]$, it is enough to see that

$$(r_1,\ 0) + (r_2,\ 0) = (r_1 + r_2,\ 0) \in S,$$

$$(r_1,\ 0)(r_2,\ 0) = (r_1r_2 - 0,\ r_10 + r_20) = (r_1r_2,\ 0) \in S,$$

and that they have the same identity element: $1_S = 1_{R[i]} = (1_R,\ 0_R)$.

Now let us define the following map

$$f :\ R \longrightarrow S,\quad f(r) = (r,\ 0).$$

It is fairly straightforward to check that f is an isomorphism between R and S, left to you.(look at the solutions for problems 4 and 6.)

And for the last part, put $i := (0,\ 1_R)$. Now since f is an isomorphism between R and its image in $R[i]$ under f, we can identify any element $r \in R$ with its image $(r,\ 0)$ in $R[i]$. Now notice that under this identification

$$i^2 = (0,\ 1)(0,\ 1) = (-1,\ 0) = -1.$$

Solution of the problem 10. Under the identification as above, any element $(x,\ y)$ of $\mathbb{R}[i]$ can be viewed as a complex number:

$$(x,\ y) = (x,\ 0) + (0,\ y) = (x,\ 0) + (0,\ 1)(y,\ 0) = x + iy.$$

Note that in $R[i]$, the letter i stands for the element $(0,\ 1)$, whereas in $x + iy$, the same letter stands for the usual imaginary number $\sqrt{-1}$. To make all these precise, we define the map

$$f:\ \mathbb{R}[i] \longrightarrow \mathbb{C}, \quad f(x,\ y) = x + iy.$$

Once again this is just the matter of a simple verification that f provides an isomorphism between the ring $\mathbb{R}[i]$ (as defined in the previous problem) and the field of complex numbers $\mathbb{C}$. CHECK THIS!

Solution of the problem 11. We define the right map and verify that it respects multiplication and you check the rest. Namely, check that it is bijective, it sends $1_{\mathbb{C}[i]}$ to $1_{\mathbb{C}\times\mathbb{C}}$, and it also respects addition.

Define

$$f:\ \mathbb{C}[i] \longrightarrow \mathbb{C}\times\mathbb{C}, \quad f(\alpha,\ \beta) = (\alpha + \sqrt{-1}\beta,\ \alpha - \sqrt{-1}\beta).$$

For any two pairs $(\alpha,\ \beta)$ and $(\alpha',\ \beta')$ in $\mathbb{C}[i]$, we have

$$\begin{aligned} f(\alpha,\ \beta)f(\alpha',\ \beta') &= (\alpha + \sqrt{-1}\beta,\ \alpha - \sqrt{-1}\beta)(\alpha' + \sqrt{-1}\beta',\ \alpha' - \sqrt{-1}\beta') \\ &= \big((\alpha\alpha' - \beta\beta') + \sqrt{-1}(\alpha\beta' + \alpha'\beta),\ (\alpha\alpha' - \beta\beta') - \sqrt{-1}(\alpha\beta' + \alpha'\beta)\big) \\ &= f(\alpha\alpha' - \beta\beta',\ \alpha\beta' + \alpha'\beta) \\ &= f((\alpha,\ \beta)(\alpha',\ \beta')) \end{aligned}$$

Now it's your turn!

Solution of the problem 12. All we have to do is to show that every non-zero element $a \in R$ has an inverse in R. To this end, consider the following map

$$f:\ R \longrightarrow R, \quad f(r) = ar.$$

We claim that f is one-to-one:

$$f(r) = f(s) \Rightarrow ar = as \Rightarrow r = s.$$

(Remember, we are in an integral domain, so the cancellation law holds.) Since R is assumed to be finite, then every one-to-one map from R to itself is onto. This implies that 1 is in the range of f, i.e., there exists an element $b \in R$ such that $f(b) = ab = 1$, so a has inverse and we are done.