Homework

Jon Allen

December 10, 2014

Section 5.1: 4 Section 5.2: 18 Section 5.3: 11, 17.

5.1 4. Let $R = \{m + n\sqrt{2} : m, n \in \mathbb{Z}\}$

(a) Show that $m + n\sqrt{2}$ is a unit in R if and only if $m^2 - 2n^2 = \pm 1$.
Hint: Show that if $(m + n\sqrt{2})(x + y\sqrt{2}) = 1$ then $(m - n\sqrt{2})(x - y\sqrt{2}) = 1$ and multiply the two equations.
Assume that $m + n\sqrt{2}$ is a unit in R. Then we can find some $x + y\sqrt{2}$ such that

$$\begin{aligned}(m + n\sqrt{2})(x + y\sqrt{2}) = mx + \sqrt{2}(my + nx) + 2ny &= 1 \\ mx - 2ny &= 1\end{aligned}$$

Note that $my + nx$ has to be 0 (the reals are an integral domain, and we have an integer [rational] result).

$$\begin{aligned}(m - n\sqrt{2})(x - y\sqrt{2}) &= mx - \sqrt{2}(my + nx) + 2ny \\ &= mx + 2ny = 1 \\ (m - n\sqrt{2})(x - y\sqrt{2})(m + n\sqrt{2})(x + y\sqrt{2}) &= 1 \\ (m^2 - 2n^2)(x^2 - 2y^2) &= 1\end{aligned}$$

And because we are dealing with integers, we know that $m^2 - 2n^2 = x^2 - 2y^2 = \pm 1$.
Now $m^2 - 2n^2 = \pm 1 = (m + n\sqrt{2})(m - n\sqrt{2})$ and so $m + n\sqrt{2}$ has an inverse of either $m - n\sqrt{2}$ or $-m + n\sqrt{2}$. $\square$

(b) Show that $1 + 2\sqrt{2}$ has infinite order in $R^\times$
If $1 + 2\sqrt{2}$ doesn't have infinite order, then there exists some n such that $(1 + 2\sqrt{2})^n = 1 = (1 + 2\sqrt{2})(1 + 2\sqrt{2})^{n-1}$. I don't know what $(1 + 2\sqrt{2})^{n-1}$ is but if it exists, then it is the inverse of $1 + 2\sqrt{2}$ which would make $1 + 2\sqrt{2}$ a unit. And so we know $1^2 - 2 \cdot 2^2 = \pm 1$. Whoops, guess it's not a unit, and therefore has infinite order.

(c) Show that 1 and -1 are the only units that have finite order in $R^\times$
We take a finite order element $(m + n\sqrt{2})$ and note that if it has finite order, then it has an inverse and so $m^2 - 2n^2 = \pm 1$ and so $m^2 = n^2 + 1$ or $n^2 = m^2 + 1$. We assume that $m^2 = n^2 + 1$. And so $n^2 + 1 = m^2 > n^2 \therefore |m| \geq |n| + 1 > |n|$. Now $(|n| + 1)^2 = n^2 + 2|n| + 1$ gives us $n^2 + 1 \geq n^2 + 2|n| + 1$ and $0 \geq |n|$. So we know that $m^2 = \pm 1$ and then $m = \pm 1$ as expected. Doing the same trick the other way around we get $0 = m$ and then $-2n^2 = \pm 1$. Which means that $(\pm 2)^{-1} = n^2$. Obviously ± 2 has no inverse in $\mathbb{Z}$ and $n^2 \in \mathbb{Z}$ so the only finite order elements are 1 and -1.

5.2 18. Define $\phi : \mathbb{Z} \to \mathbb{Z}_m \oplus \mathbb{Z}_n$ by $\phi(x) = ([x]_m, [x]_n)$. Find the kernel and image of ϕ. Show that ϕ is onto if and only if $\gcd(m, n) = 1$.
If $[x]_m = [0]_m$ then $m|x$ and similarly if $[x]_n = [0]_n$ then $n|x$. Then $\ker(\phi) = \{x \in \mathbb{Z} : m|x \text{ and } n|x\}$.

Let $k = \gcd(m,n)$ and $m = ka, n = kb$. Then $[x]_k = [mq + [x]_m]_k = [kaq + [x]_m]_k = [[x]_m]_k$ and similarly $[x]_k = [[x]_n]_k$ and so $[[x]_m]_k = [[x]_n]_k$. So the image consists of $\{(x,y) \in \mathbb{Z}_m \oplus \mathbb{Z}_n : [x]_{\gcd(m,n)} = [y]_{\gcd(m,n)}\}$.
Now if $\gcd(m,n)$ is one then there are no restrictions on the image and so it is onto. That is to say $[x]_1 = [0]_1$ regardless of ones choice of x. If $\gcd(m,n) = k > 1$ then $0 \in \mathbb{Z}_m$ and $1 \in \mathbb{Z}_n$. Now $k > 1$ and so $[[0]_m]_k = [0]_k \neq [1]_k = [[1]_n]_k$. And so $([0]_m, [1]_n) \notin \phi(\mathbb{Z})$ and then ϕ is not onto.

5.3 11. Let R be a commutative ring, with $a \in R$. The **annihilator** of a is defined by

$$\mathrm{Ann}(a) = \{x \in R : xa = 0\}$$

Prove that $\mathrm{Ann}(a)$ is an ideal of R

proof

Let us take any $x, y \in \mathrm{Ann}(a)$. Then $(x+y)a = xa + ya = 0$ and so $x + y \in \mathrm{Ann}(a)$. Similarly $(x-y)a = xa - ya = 0$ and so $x \pm y \in \mathrm{Ann}(a)$. Now if we take an arbitrary $r \in R$ and an arbitrary $x \in \mathrm{Ann}(a)$ then $(rx)a = r(xa) = r0 = 0$ and so $rx \in \mathrm{Ann}(a)$. $\square$

17. Let R be the set of all matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ over $\mathbb{Q}$ such that $a = d$ and $c = 0$.

So $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$

(a) Verify that R is a commutative ring.
We get that addition is an abelian group for free because the elements of the matrices are in $\mathbb{Q}$ which is an abelian group.

$$\begin{bmatrix} a_1 & b_1 \\ 0 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ 0 & a_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 & a_1b_2 + a_2b_1 \\ 0 & a_1a_2 \end{bmatrix}$$

Because $\mathbb{Q}$ is commutative under multiplication and addition, it is easy to see that that above multiplication is also commutative (swapping the ones and twos doesn't change anything). Now changing a_2 to $a_2 + a_3$ and likewise $b_2 \Rightarrow b_2 + b_3$ the above result becomes

$$\begin{bmatrix} a_1(a_2+a_3) & a_1(b_2+b_3) + (a_2+a_3)b_1 \\ 0 & a_1(a_2+a_3) \end{bmatrix} = \begin{bmatrix} a_1a_2 & a_1b_2 + a_2b_1 \\ 0 & a_1a_2 \end{bmatrix} + \begin{bmatrix} a_1a_3 & a_1b_3 + a_3b_1 \\ 0 & a_1a_3 \end{bmatrix}$$

Which give us distribution for multiplication, so we have a commutative ring.

(b) Let I be the set of all such matrices for which $a = d = 0$. Show that I is an ideal of R.
Obviously $\begin{bmatrix} 0 & b_1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & b_2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & b_1 + b_2 \\ 0 & 0 \end{bmatrix} \in I$ and $\begin{bmatrix} a & b_1 \\ 0 & a \end{bmatrix} \begin{bmatrix} 0 & b_2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & ab_2 \\ 0 & 0 \end{bmatrix}$.
Because $ab_2 \in \mathbb{Q}$ then $\begin{bmatrix} 0 & ab_2 \\ 0 & 0 \end{bmatrix} \in I$

(c) Use the fundamental homomorphism theorem for rings to show that $R/I \cong \mathbb{Q}$.
$\phi : \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \to a$

$$\phi\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) = 1$$

$$\phi\left(\begin{bmatrix} a_1 & b_1 \\ 0 & a_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ 0 & a_2 \end{bmatrix}\right) = a_1 + a_2$$

$$
\begin{aligned}
&= \phi\left(\begin{bmatrix} a_1 & b_1 \\ 0 & a_1 \end{bmatrix}\right) + \phi\left(\begin{bmatrix} a_2 & b_2 \\ 0 & a_2 \end{bmatrix}\right) \\
\phi\left(\begin{bmatrix} a_1 & b_1 \\ 0 & a_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ 0 & a_2 \end{bmatrix}\right) &= a_1 a_2 \\
&= \phi\left(\begin{bmatrix} a_1 & b_1 \\ 0 & a_1 \end{bmatrix}\right) \phi\left(\begin{bmatrix} a_2 & b_2 \\ 0 & a_2 \end{bmatrix}\right) \\
\phi\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} &= 0
\end{aligned}
$$

So we see that ϕ is a homomorphism and I is $\ker\phi$
Clearly $\phi(R) = \mathbb{Q}$ as we have no restriction on the "a" element. And so by the fundamental homomorphism theorem for rings we have $R/I \cong \mathbb{Q}$