Homework 1 (Due Jan 22, 2025)

Jack Hyatt
MATH 547 - Algebraic Structures II - Spring 2025

June 8, 2025

Justify all of your answers completely.

1. Let R be a ring and let $S = R[[X]]$ be the ring of formal power series with coefficients in R. Let $f = \sum_{n=0}^{\infty} a_n X^n$ be an element in S, where $a_n \in R$ for all $n \geq 0$. Prove that f is a unit in S if and only if a_0 is a unit in R.

   Proof. ($\implies$)
   Assume f is a unit in S. Then let us denote $f^{-1} = \sum_{n=0}^{\infty} a'_n X^n$ as the multiplicative inverse of f.
   $$1 = ff^{-1} = \sum_{n=0}^{\infty} (\sum_{k=0}^{n} a_k a'_{n-k}) X^n$$
   So then $\sum_{k=0}^{n} a_k a'_{n-k} = 0$ for every $n \neq 0$ and $a_0 a'_0 = 1$. A similar argument can be made for $a'_0 a_0 = 1$, meaning that a'_0 is the inverse of a_0, making a_0 a unit in R.

   ($\impliedby$)
   Let $f = \sum_{n=0}^{\infty} a_n X^n$ be an element in S, where $a_n \in R$ for all $n \geq 0$. Assume a_0 is a unit in R. Then let us denote a_0^{-1} as the multiplicative inverse of a_0.

   Now to construct $f^{-1} = \sum_{n=0}^{\infty} a'_n X^n$. We would need $1 = ff^{-1} = \sum_{n=0}^{\infty} b_n X^n$, having $b_n = \sum_{k=0}^{n} a_n a'_{n-k}$. We want $b_0 = 1$ and $b_i = 0$ for $i > 0$. So clearly let $a'_0 = a_0^{-1}$ to get $b_0 = 1$.

   For a'_n where $n > 0$, we construct recursively with
   $$0 = \sum_{k=0}^{n} a_n a'_{n-k} \implies 0 = a_0 a'_n + \sum_{k=1}^{n} a_n a'_{n-k} \implies a'_n = -a_0^{-1} \sum_{k=1}^{n} a_n a'_{n-k}.$$

   This is well defined, as every a'_n will be constructed with a sum of finite terms, all of which defined in sequence.

   We have now defined every a'_n so that $ff^{-1} = 1$, making f a unit in S. ∎

2. Let S be a ring, let R be a subring of S, and let u be a fixed element of S which is not in R. Consider

$$T = \{a + bu : a, b \in R\}$$

Prove that T is a subring of S if and only if there exists a monic polynomial $f(X) \in R[x]$ of degree 2 with $f(u) = 0$.

Proof. $(\implies)$
Assume T is a subring of S. Since R is a subring, we have the same zero and one elements, denoting 0 and 1, in R. So then $u \in T$.

Since T is a subring, it is closed under multiplication. So $u^2 = a' + b'u$ for some $a', b' \in R$.

It is now easy to see that the following monic of degree 2 is equal to 0 when evaluated at u.

$$f(x) = x^2 - b'x - a'$$

$(\impliedby)$
Assume $f(X) \in R[x]$ is a monic polynomial of degree 2 with $f(u) = 0$, denoted $f(x) = x^2 - b'x - a'$ for some $a', b' \in R$. Then we can also say $u^2 = b'u + a'$.

First, it is obvious that every element of $T = \{a + bu : a, b \in R\}$ is also in S. It is also clear that T is closed under addition since R is a subring and also closed under addition and multiplication. It is less clear for multiplication.

Let $a_1 + b_1u$ and $a_2 + b_2u$ be elements of T. Then

$$\begin{aligned}(a_1 + b_1u)(a_2 + b_2u) &= (a_1a_2) + (a_1b_2 + b_1a_2)u + b_1b_2u^2 \\ &= (a_1a_2) + (a_1b_2 + b_1a_2)u + b_1b_2(b'u + a')\end{aligned}$$

which will clearly be in T as R is closed under addition and multiplication. So T is closed under multiplication.

Finally, T also contains 1 since R also contains 1. So T is a subring of S. ∎

3. For each of the following, decide whether the set

$$T = \{a + bu : a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{R}$ or not. Justify your answers. You may use the result from problem 2.

(a) $u = 1 + \sqrt{2}$

We have

$$T = \{a + b(1 + \sqrt{2}) : a, b \in \mathbb{Z}\}$$

Check u^2:

$$(1 + \sqrt{2})^2 = 3 + 2\sqrt{2} = 1 + 2 + 2\sqrt{2} = 1 + 2(1 + \sqrt{2})$$

So then we could construct a monic degree 2 polynomial with $f(u) = 0$, following the same idea as the forward direction in proof of problem 2. So T is a subring.

(b) $u = (1+\sqrt{3})/2$ We have

$$T = \left\{ a + b\left(\frac{1+\sqrt{3}}{2}\right) : a, b \in \mathbb{Z} \right\}$$

Consider $u \cdot u$:

$$\left(\frac{1+\sqrt{3}}{2}\right)^2 = 1 + \frac{\sqrt{3}}{2} = \frac{1}{2} + \left(\frac{1+\sqrt{3}}{2}\right) \notin T$$

So T is not closed under multiplication, making it not a subring.

4. Let $R = \{a + bi : a, b \in \mathbb{Z}\}$. It is easy to check that R is a subring of $\mathbb{C}$ (don't do). Consider the function $\Phi : R \to \mathbb{Z}$ defined by $\Phi(a + bi) = a^2 + b^2$.

(a) Prove that $a + bi$ is a unit in R if and only if $\Phi(a + bi) = 1$.

Proof. $(\implies)$
Assume $a + bi$ is a unit in R. Denote $c + di$ as its multiplicative inverse.

$$1 = (a + bi)(c + di) = ac + (ad + bc)i - bd \implies$$

$$1 = ac - bd \qquad 0 = ad + bc$$

Seeing $ac - bd$ gives the idea of using matrices. We then can have

$$\begin{aligned} ac - bd &= 1 \\ ad + bc &= 0 \end{aligned}$$

giving

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

For that system to have $(c, d) \in \mathbb{Z}^2$ as a solution, the determinant of $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ must be ± 1, making sure the matrix is invertible over the integers.
So then $\det\left(\begin{bmatrix} a & -b \\ b & a \end{bmatrix}\right) = a^2 + b^2 = 1$ since squares of integers can never be negative.
$(\impliedby)$
Assume $\Phi(a+bi) = 1$. So then $a^2+b^2 = 1$. So then we have $(a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$ since $a, b \in \mathbb{Z}$. This gives a list of possible values for $a + bi$ being $1, -1, i, -i$.
To check if the elements are units: 1 and -1 are their own multiplicative inverses, while i and $-i$ are multiplicative inverses of each other. ■

(b) Use the result from part a. to find all the units in R.

The reverse direction of the proof lists outs that the only units are $-1, 1, -i, i$.