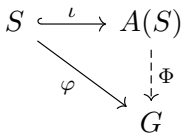
Abstract Algebra I Homework 5

Carson Connard

Section 6.3

11 Let S be a set. The group with presentation (S, R), where $R = \{[s,t] : s,t \in S\}$ is called the *free abelian* group on S, which we denote as $A(S)$. Prove that $A(S)$ has the following universal property: if G is any abelian group and $\varphi : S \to G$ is any set map, then there is a unique group homomorphism $\Phi : A(S) \to G$ such that $\Phi|_S = \varphi$. Deduce that if A is a free abelian group on a set of cardinality n then $A \cong \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ (n factors).

Proof. First notice that since S generates G, we have the inclusion mapping $\iota : S \hookrightarrow A(S)$. So, we aim to show that there exists some Φ such that the following diagram commutes:



So, consider $A(S)$ to be the free group generated by S, and consider $\varphi : S \to G$ as in the problem statement. Since $A(S)$ is freely generated, we know that every element $a \in A(S)$ can be written as a word of the following form:

$$a = s_{i_1}^{k_1} \cdots s_{i_n}^{k_n} \quad \text{for} \quad s_{i_j \in S} \text{ and } k_i \in \{\pm 1\}.$$

Let us then define the map $\Phi : A(S) \to G$ as $\Phi(a) = (\varphi(s_{i_j}))^{k_1} \cdot (\varphi(s_{i_n}))^{k_n}$. We aim to show that Φ is a homomorphism. So, take arbitrary words $a, b \in A(S)$, which we write as

$$a = y_1 \cdots y_n z_1 \cdots z_m \text{ and } b = z_m^{-1} \cdots z_1^{-1} y_{n+1} \cdots y_k, \text{ where } y_i, z_j \in S,\ y_n \neq y_{n+1}^{-1}.$$

Certainly then $ab = y_1 \cdots y_n y_{n+1} \cdots y_k$ is a reduced word in S. Finally, we see

$$\begin{aligned} \Phi(ab) &= \Phi(y_1) \cdots \Phi(y_n)\Phi(y_{n+1}) \cdots \Phi(y_k) \\ &= \Phi(y_1) \cdots \Phi(y_n)\Phi(z_1) \cdots \Phi(z_m)\Phi(z_m)^{-1} \cdots \Phi(z_1)^{-1}\Phi(y_{n+1}) \cdots \Phi(y_k) \\ &= \Phi(a)\Phi(b), \end{aligned}$$

which gives that Φ is indeed a homomorphism. We see that indeed, the diagram above then commutes, since $\Phi \circ \iota = \varphi$. Since Φ is defined off of words in $A(S)$, and since each element $a \in A(S)$ has a unique word representation, we must have that Φ is unique. □

Section 7.1

5 Decide which of the following are subrings of $\mathbb{Q}$:

(a) The set of all rational numbers with odd denominators (when written in lowest terms).

Proof. First, we aim to show that this set (which we will refer to as A) is a subgroup of $(\mathbb{Q}, +)$. So, first consider $a/b,\ c/d \in A$, that is b, d are odd. Then

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Since the product of two odd numbers is also odd, we have closure under addition. Next, associativity is certain to hold since it holds within $\mathbb{Q}$, and $A \subset \mathbb{Q}$. Next, we see that $0/1$ is identity, that is

$$\frac{0}{1} + \frac{a}{b} = \frac{a}{b} = \frac{a}{b} + \frac{0}{1} \quad \forall a, b \in A.$$

Finally, consider a/b and $-a/b$ as elements of A. We see that

$$\frac{a}{b} + \frac{-a}{b} = \frac{0}{b} = \frac{0}{1} \quad \text{and} \quad \frac{-a}{b} + \frac{a}{b} = \frac{0}{b} = \frac{0}{1}.$$

So, since a was taken arbitrarily, we have that every element has an inverse. So $(A, +) \subset (\mathbb{Q}, +)$.

Now, we aim to show closure under multiplication. Consider $a/b,\ c/d \in A$, that is b, d are odd, which implies bd is odd. So, multiplying these elements yields the element $\frac{ac}{bd}$, which when reduced to lowest terms must have a denominator which divides bd, which means that said reduced denominator must also be odd. So, we have closure under multiplication, and therefore we see that A is a subring of $\mathbb{Q}$. □

(b) The set of all rational numbers with even denominators (when written in lowest terms).

Solution. Consider the following counterexample:

$$\frac{1}{6} + \frac{1}{6} = \frac{1}{3}.$$

We see that the set described is not a subring of $\mathbb{Q}$ since addition is not closed.

(c) The set of all nonnegative rational numbers.

Solution. Notice that in this set, the only element with an additive inverse is 0, and therefore we see that this set is not a subring of $\mathbb{Q}$; further, it is not even a subgroup.

(d) The set of squares of rational numbers.

Solution. Consider the following counterexample: certainly 1 is an element of the set, as $1 = 1^2$. However, we do not have closure under addition since $1 + 1 = 2$, and $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$. So, this set is not a subring of $\mathbb{Q}$.

(e) The set of all rational numbers with odd numerators (when written in lowest terms).

Solution. Consider the following counterexample: certainly $1/3$ is in the set, however the sum $1/3 + 1/3 = 2/3$ is not in the set, even with it already being reduced fully. So, this set is not a subring of $\mathbb{Q}$.

(f) The set of all rational numbers with even numerators (when written in lowest terms).

Proof. First, we aim to show that this set (which we will refer to as F) is a subgroup of $(\mathbb{Q}, +)$. Consider elements $a/b,\ c/d \in F$, that is a, c are even. Then we have that

$$\frac{a}{b} + \frac{-c}{d} = \frac{ad - bc}{bd}.$$

We must have that b and d are odd, otherwise we could factor out a power of 2 from both the numerator and denominator, which would remove the evenness of the numerator. So, we have then that $(ad - bc)/bd \in F$. The additive identity and inverse follow in similar fashion to part (a), giving that F is a subgroup of $(\mathbb{Q}, +)$.

Now we aim to show closure under multiplication. Take again $a/b,\ c/d \in F$, then we have that b, d are odd. It follows then that $2 \mid ac$. So, indeed we have that $ac/bd \in F$, and F is closed under multiplication. So, F is a subring of $\mathbb{Q}$. □

26 Let K be a field. A *discrete valuation* on K is a function $\nu : K^\times \to \mathbb{Z}$ satisfying (i) $\nu(ab) = \nu(a) + \nu(b)$ (i.e. ν is a homomorphism from the multiplicative group of nonzero elements of K to $\mathbb{Z}$); (ii) ν is surjective; (iii) $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$ for all $x, y \in K^\times$ with $x + y \neq 0$.
The set $R = \{x \in K^\times : \nu(x) \geq 0\} \cup \{0\}$ is called the *valuation ring* of ν.

(a) Prove that R is a subring of K which contains the identity.

Proof. By definition $0 \in R$, so $R \neq \emptyset$. Take arbitrary $x, y \in R$. Then if $x \neq 0$ but $y = 0$, then $\nu(x, y) = \nu(x) \geq 0$, and similarly if $x = 0$ but $y \neq 0$, then $\nu(x, y) = \nu(-y) = \nu(y) \geq 0$. Note that the equality $\nu(y) = \nu(-y)$ follows from the definition of ν, that is

$$\begin{aligned} \nu(x) = \nu(1 \cdot x) = \nu(1) + \nu(x) &\implies 0 = \nu(1) = \nu((-1)(-1)) = \nu(-1) + \nu(-1) \\ &\implies \nu(-1) = -\nu(-1) = 0 \\ &\implies \nu(-x) = \nu((-1)x) = \nu(-1) + \nu(x) = \nu(x). \end{aligned}$$

Continuing, we have that $\nu(x), \nu(y) \geq 0$. Consider the case in which $x = y = 0$. Then $x - y = 0 \in R$. Consider the case in which $x, y \neq 0$, then we have that either $x - y = 0 \in R$ or $x - y \neq 0$. Then we have that $\nu(x - y) \geq \min(\nu(x), \nu(-y)) = \min(\nu(x), \nu(y)) \geq 0$. Finally consider xy. If $xy = 0$ then $xy \in R$, otherwise $\nu(xy) = \nu(x) + \nu(y) \geq 0$, and therefore $xy \in R$ still. So, R is a subring of K. Moreover $1 \in R$ since $\nu(1) = 0$ as shown in our aside. □

(b) Prove that for each nonzero element $x \in K$, either x or x^{-1} is in R.

Proof. Suppose $0 \neq x \in K$. Then $0 = \nu(1) = \nu(xx^{-1}) = \nu(x) + \nu(x^{-1})$. Then $\nu(x) = -\nu(x^{-1})$, so either $\nu(x)$ or $\nu(x^{-1})$ is nonnegative, not both as desired. □

(c) Prove that an element x is a unit of R if and only if $\nu(x) = 0$.

Proof. Take $x \in R$ to be a unit. Then by definition $x^{-1} \in R$. Earlier we saw that $\nu(a) = -\nu(a^{-1})$, and that both $\nu(a)$ and $\nu(a^{-1})$ are nonnegative, implying that we must have that $\nu(a) = \nu(a^{-1}) = 0$.
Now consider $\nu(x) = 0$, then $\nu(x^{-1}) = -\nu(x) = 0$. So, $x^{-1} \in R$ and then we must have that $x \in R$ is a unit. □

Section 7.2

3 Define the set $R[[x]]$ of *formal power series* in the indeterminate x with coefficients from R to be all formal infinite sums

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots .$$

Define addition and multiplication of power series in the same way as for power series with real or complex coefficients, that is extend polynomial addition and multiplication to power series as through they were "polynomials of infinite degree":

$$\begin{aligned} \sum_{n=0}^{\infty} a_n x^n \ + \ \sum_{n=0}^{\infty} b_n x^n &= \sum_{n=0}^{\infty} (a_n + b_n) x^n, \\ \sum_{n=0}^{\infty} a_n x^n \ \times \ \sum_{n=0}^{\infty} b_n x^n &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n. \end{aligned}$$

(The term "formal" is used here to indicate that convergence is not considered, so that formal power series need not represent functions on $\mathbb{R}$).

(a) Prove that $R[[x]]$ is a commutative ring with identity.

Proof. First we show associativity of addition:

$$\begin{aligned}\left(\left(\sum_{n=0}^{\infty} a_n x^n\right) + \left(\sum_{n=0}^{\infty} b_n x^n\right)\right) + \left(\sum_{n=0}^{\infty} c_n x^n\right) &= \left(\sum_{n=0}^{\infty} (a_n + b_n) x^n\right) + \left(\sum_{n=0}^{\infty} c_n x^n\right) \\ &= \sum_{n=0}^{\infty} ((a_n + b_n) + c_n) x^n \\ &= \sum_{n=0}^{\infty} (a_n + (b_n + c_n)) x^n \\ &= \left(\sum_{n=0}^{\infty} a_n x^n\right) + \left(\sum_{n=0}^{\infty} (b_n + c_n) x^n\right) \\ &= \left(\sum_{n=0}^{\infty} a_n x^n\right) + \left(\left(\sum_{n=0}^{\infty} b_n x^n\right) + \left(\sum_{n=0}^{\infty} c_n x^n\right)\right).\end{aligned}$$

Now denote $0 = \sum_{n=0}^{\infty} 0 \cdot x^n$. We see 0 is an additive identity by the following:

$$\sum_{n=0}^{\infty} a_n x^n \ + \ \sum_{n=0}^{\infty} 0 \cdot x^n = \sum_{n=0}^{\infty} (a_n + 0) x^n = \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} (0 + a_n) x^n = \sum_{n=0}^{\infty} 0 \cdot x^n \ + \ \sum_{n=0}^{\infty} a_n x^n.$$

Now consider $\sum_{n=0}^{\infty} (-a_n) x^n$. We see that this is an additive inverse by the following:

$$\sum_{n=0}^{\infty} a_n x^n \ + \ \sum_{n=0}^{\infty} (-a_n) x^n = \sum_{n=0}^{\infty} (a_n - a_n) x^n = \sum_{n=0}^{\infty} 0 \cdot x^n = 0.$$

Now to show commutativity of addition, we see the following:

$$\sum_{n=0}^{\infty} a_n x^n \ + \ \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n = \sum_{n=0}^{\infty} (b_n + a_n) x^n = \sum_{n=0}^{\infty} b_n x^n \ + \ \sum_{n=0}^{\infty} a_n x^n.$$

So, all desired properties for addition hold.

Now, we aim to show associativity and distributivity of multiplication. First, associativity is seen via the following:

$$\begin{aligned}\left(\left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right)\right)\left(\sum_{n=0}^{\infty} c_n x^n\right) &= \left(\sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i b_j\right) x_n\right)\left(\sum_{n=0}^{\infty} c_n x^n\right) \\ &= \sum_{n=0}^{\infty} \left(\sum_{t+k=n} \left(\sum_{i+j=t} a_i b_j\right) c_k\right) x^n \\ &= \sum_{n=0}^{\infty} \left(\sum_{t+k=n} \sum_{i+j=t} a_i b_j c_k\right) x^n \\ &= \sum_{n=0}^{\infty} \left(\sum_{i+j+k=n} a_i b_j c_k\right) x^n \\ &= \sum_{n=0}^{\infty} \left(\sum_{i+s=n} \sum_{j+k=s} a_i b_j c_k\right) x^n\end{aligned}$$

$$= \sum_{n=0}^{\infty} \left(\sum_{i+s=n} a_i \left(\sum_{j+k=s} b_j c_k \right) \right) x_n$$
$$= \left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} \left(\sum_{j+k=n} b_j c_k \right) x^n \right)$$
$$= \left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\left(\sum_{n=0}^{\infty} b_n x^n \right) \left(\sum_{n=0}^{\infty} c_n x^n \right) \right).$$

Next, we see that we have multiplicative distributivity on the left by the following (right distributivity is almost identical):

$$\left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\left(\sum_{n=0}^{\infty} b_n x^n \right) + \left(\sum_{n=0}^{\infty} c_n x^n \right) \right) = \left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} (b_n + c_n) x^n \right)$$
$$= \sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i (b_j + c_j) \right) x^n$$
$$= \sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i b_j + a_i c_j) \right) x^n$$
$$= \sum_{n=0}^{\infty} \left(\left(\sum_{i+j=n} a_i b_j \right) + \left(\sum_{i+j=n} a_i c_j \right) \right) x^n$$
$$= \left(\sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i b_j \right) x^n \right) + \left(\sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i c_j \right) x^n \right)$$
$$= \left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} b_n x^n \right) + \left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} c_n x^n \right).$$

We have established that $R[[x]]$ is a ring. We now want to show that it is commutative. So, take R to be commutative, and we have that $R[[x]]$ is also commutative by the following:

$$\left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i b_j \right) x^n = \sum_{n=0}^{\infty} \left(\sum_{j+i=n} b_j a_i \right) x^n = \left(\sum_{n=0}^{\infty} b_n x^n \right) \left(\sum_{n=0}^{\infty} a_n x^n \right).$$

Moreover, there exists a multiplicative identity, which we claim to be $1 := \sum_{n=0}^{\infty} e_n x^n$ where $e_0 = 1$ and $e_{n \neq 0} = 0$. Indeed, we see

$$\left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} e_n x^n \right) = \sum_{n=0}^{\infty} \left(\sum_{i+j=n}^{\infty} a_i e_j \right) x^n = \sum_{n=0}^{\infty} a_n e_0 x^n = \sum_{n=0}^{\infty} a_n x^n.$$

Again, the case for left multiplication is nearly identical. So, we see that indeed there is a multiplicative identity in $R[[x]]$. □

(b) Show that $1 - x$ is a unit in $R[[x]]$ with inverse $1 + x + x^2 + \cdots$.

Proof. Let us denote $1 - x = \sum_{n=0}^{\infty} d_n x^n$, where $d_0 = 1$, $d_1 = -1$, and any further $d_n = 0$. We see the following:

$$(1 - x) \sum_{n=0}^{\infty} x^n = \left(\sum_{n=0}^{\infty} d_n x^n \right) \left(\sum_{n=0}^{\infty} x^n \right) = \sum_{n=0}^{\infty} \left(\sum_{i+j=n} d_i \right) x^n.$$

If $n \geq 1$ then $\sum_{i+j=n} d_i = 0$ and $d_0 = 1$, and so $(1 - x) \sum_{n=0}^{\infty} x^n = 1$ as desired. □

(c) Prove that $\sum_{n=0}^{\infty} a_n x^n$ is a unit in $R[[x]]$ if and only if a_0 is a unit in R.

Proof. ($\Longrightarrow$) Let $S = \sum_{n=0}^{\infty} a_n x^n$ be a unit with inverse $S^{-1} = \sum_{n=0}^{\infty} \bar{a}_n x^n$. Then

$$SS^{-1} = \left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} \bar{a}_n x^n\right) = \sum_{n=0}^{\infty}\left(\sum_{i+j=n} a_i \bar{a}_j\right) x^n.$$

When $n = 0$, we see that $a_0\bar{a}_0 = 1$ is the coefficient of x^0. So, we have the desired result.

($\Longleftarrow$) Conversely, take a_0 to be a unit, that is $a_0\bar{a}_0 = \bar{a}_0 a_0$. Let $\bar{S} = \sum_{n=0}^{\infty} b_n x^n$ where $b_0 = \bar{a}_0$ and $b_{k+1} = -\bar{a}_0 \sum_{i+j=k+1} a_i b_j$. Then we have

$$S\bar{S} = \left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty}\left(\sum_{i+j=n} a_i b_j\right) x^n.$$

If $n = 0$, then $\sum a_i b_j = a_0\bar{a}_0 = 1$. If $n \geq 1$, then

$$\sum_{i+j=n} a_i b_j = a_0 b_n + \sum_{i+j=n} a_i b_j = a_0\left(-\bar{a}_0 \sum_{i+j=n} a_i b_j\right) + \left(\sum_{i+j=n} a_i b_j\right) = 0.$$

So, we see that $S\bar{S} = 1$. The same follows for the left inverse, and therefore S is a unit of $R[[x]]$. □

5 Let F be a field and define the ring $F((x))$ of *formal Laurent series* with coefficients in F by

$$F((x)) = \left\{ \sum_{n \geq N}^{\infty} a_n x^n : a_n \in F,\ N \in \mathbb{Z} \right\}.$$

(Every element of $F((x))$ is a power series in x plus a polynomial in $1/x$, that is each element of $F((x))$ has only a finite number of terms with negative powers of x.)

(a) Prove that $F((x))$ is a field.

Proof. We shall prove the properties of a field. First, we show that $F((x))$ is an abelian group under $(+)$. Consider lower bounds N, M for indices of summation, and we have the following:

$$\sum_{n \geq N} a_n x^n \ + \ \sum_{n \geq M} b_n x^n = \sum_{n \geq \min(N,M)} (a_n + b_n) x^n \quad \text{and} \quad \sum_{n \geq M} b_n x^n \ + \ \sum_{n \geq N} a_n x^n = \sum_{n \geq \min(N,M)} (b_n + a_n) x^n.$$

Since $a_i, b_i \in F$, the sums are equal. Associativity and closure of $(+)$ follow from the properties of polynomials. Also, the additive inverse of some $\sum a_n x^n$ is identified as $\sum(-a_n)x^n$, and the identity element is $0 = \sum 0x^n$.

Next, we aim to show that $(\cdot)$ is distributive over addition and is commutative. Taking L as a lower bound for indexing a sum, we certainly have:

$$\sum_{n \geq N} a_n x^n \left(\sum_{n \geq M} b_n x^n + \sum_{n \geq L} c_n x^n\right) = \sum_{n \geq N} a_n x^n \left(\sum_{n \geq \min(M,L)} (b_n + c_n) x^n\right).$$

Then each coefficient of the product is of the form $a_j(b_i + c_i)$, which we know can be rewritten as $a_j b_i + a_j c_i$ since $a_j, b_i, c_i \in F$, which must have the distributive property by definition, and moreover $a_j b_i + a_j c_i = b_i a_j + c_i a_j$ by the commutative property on F.

For a multiplicative identity, the unit in F, 1_F, works.

Finally, we want multiplicative inverses. Take N to be minimal such that $a_N \neq 0$. Since F is a field, we know that a_N^{-1} exists. Define now $S = \sum_{n \geq -N} d_n x^n$ where $d_{-N} = a_n^{-1}$ and $d_{k+1} = -a_n^{-1} \sum_{i+j=k+N+1,\, j \leq k} a_i d_j$. We see the following for $\gamma \neq 0$ in $F((x))$:

$$\begin{aligned}\gamma S &= \left(\sum_{n \geq N} a_n x^n\right)\left(\sum_{n \geq -N} d_n x^n\right) \\ &= \sum_{n \geq N-N} \left(\sum_{i+j=n} a_i d_j\right) x^n \\ &= 1.\end{aligned}$$

We see that indeed this works as the form for an inverse. □

(b) Define the map

$$\nu : F((x))^\times \to \mathbb{Z} \quad \text{by} \quad \nu\left(\sum_{n \geq N}^{\infty} a_n x^n\right) = N,$$

where a_N is the first nonzero coefficient of the series (i.e. N is the "order of zero or pole of the series at 0"). Prove that ν is a discrete valuation on $F((x))$ whose discrete valuation ring is $F[[x]]$ as above.

Proof. First, we aim to show that $\nu(a+b) = \nu(a) + \nu(b)$. Suppose N, M are maximal valuations for $\nu(a)$ and $\nu(b)$ respectively, to where neither are equal to 0. Then the $N+M$th coefficient of ab is nonzero, and all previous coefficients are 0. Therefore we must have $\nu(a+b) = \nu(a) + \nu(b)$.

Second, we show that ν is surjective. Define $\eta_k \in F((x))$ by $\eta_k(n) = 1$ for $k = n$ and 0 otherwise. Then $\nu(\eta_k) = k$ and ν is surjective.

Third, we aim to show $\nu(a+b) \geq \min(\nu(a), \nu(b))$. Suppose N, M are the same as in the first part of this proof. Then if we let $P = \min(N, M)$, then $a_k = 0$ for all $k < P$. Therefore $\nu(a+b) \geq \min(\nu(a), \nu(b))$ as desired.

Finally we know that $0 \in F[[x]]$, and if $\nu(a) \geq 0$ then $a \in F[[x]]$. Conversely if $a \in F[[x]]$ then $\nu(a) \geq 0$ or $a = 0$. So, indeed $F[[x]]$ is the discrete valuation ring of $F((x))$. □

Section 7.3

12 Let D be an integer which is not a perfect square in $\mathbb{Z}$, and let $S = \left\{ \begin{pmatrix} a & b \\ Db & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$.

(a) Prove that S is a subring of $M_2(\mathbb{Z})$.

Proof. Notice first that the additive identity, $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is certainly in S. Consider the following two matrices in S:

$$A = \begin{pmatrix} a_1 & b_1 \\ Db_1 & a_1 \end{pmatrix}, \quad \begin{pmatrix} a_2 & b_2 \\ Db_2 & a_2 \end{pmatrix}.$$

Then we see that indeed,

$$A - B = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ D(b_1 - b_2) & a_1 - a_2 \end{pmatrix} \in S \quad \text{and} \quad AB = \begin{pmatrix} a_1a_2 + Db_1b_2 & a_1b_2 + b_1a_2 \\ D(a_1b_2 + b_1a_2) & a_1a_2 + Db_1b_2 \end{pmatrix} \in S,$$

so S is indeed a subring of $M_2(\mathbb{Z})$. □

(b) If D is not a perfect square in $\mathbb{Z}$, prove that the map $\phi : \mathbb{Z}[\sqrt{D}] \to S$ defined by $\phi(a + b\sqrt{D}) = \begin{pmatrix} a & b \\ Db & a \end{pmatrix}$ is a ring isomorphism.

Proof. First, note the following. We know that if D is not a perfect square, then we have that $\sqrt{D} \notin \mathbb{Q}$. If we consider the equation $a_1 + b_1\sqrt{D} = a_2 + b_2\sqrt{D}$, then we know that $a_1 = a_2$ and $b_1 = b_2$. As a short proof, suppose for the sake of contradiction that $b_1 \neq b_2$. Then $\sqrt{D} = (a_1 - a_2)/(b_2 - b_1) \in \mathbb{Q}$, which contradicts what we know about $\sqrt{D}$. $\diamond$

Consider ϕ. By the argument in the preceding paragraph, we see that ϕ must be well defined. We aim to show that ϕ is a ring homomorphism. We see the following:

$$\begin{aligned}
\phi((a_1 + b_1\sqrt{D}) + (a_2 + b_2\sqrt{D})) &= \phi((a_1 + a_2) + (b_1 + b_2)\sqrt{D}) \\
&= \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ D(b_1 + b_2) & a_1 + a_2 \end{pmatrix} \\
&= \begin{pmatrix} a_1 & b_1 \\ Db_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ Db_2 & a_2 \end{pmatrix} \\
&= \phi(a_1 + b_1\sqrt{D}) + \phi(a_2 + b_2\sqrt{D}), \\
\phi((a_1 + b_1\sqrt{D})(a_2 + b_2\sqrt{D})) &= \phi((a_1a_2 + Db_1b_2) + (a_1b_2 + a_2b_1)\sqrt{D}) \\
&= \begin{pmatrix} a_1a_2 + Db_1b_2 & a_1b_2 + a_2b_1 \\ D(a_1b_2 + a_2b_1) & a_1a_2 + Db_1b_2 \end{pmatrix} \\
&= \begin{pmatrix} a_1 & b_1 \\ Db_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ Db_2 & a_2 \end{pmatrix} \\
&= \phi(a_1 + b_1\sqrt{D})\phi(a_2 + b_2\sqrt{D}).
\end{aligned}$$

We see that indeed, ϕ is a ring homomorphism. Finally, we aim to show that ϕ is a bijection. First, ϕ is surjective because for $\begin{pmatrix} a & b \\ Db & a \end{pmatrix} \in S$, we have that $\phi(a + b\sqrt{D}) = \begin{pmatrix} a & b \\ Db & a \end{pmatrix}$. We can show injectivity by showing that $\ker\phi$ is trivial. So, take $a + b\sqrt{D} \in \ker\phi$. Then we see that

$$\phi(a + b\sqrt{D}) = \begin{pmatrix} a & b \\ Db & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0,$$

and therefore $a = b = 0$, which means that the kernel is indeed trivial. So, ϕ is a bijective ring homomorphism; a ring isomorphism. $\square$

(c) If $D \equiv 1 \bmod 4$ is squarefree, prove that the set $S := \left\{ \begin{pmatrix} a & b \\ (D-1)b/4 & a+b \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ is a subring of $M_2(\mathbb{Z})$ and is isomorphic to the quadratic integer ring $\mathcal{O}$.

Proof. First define matrices

$$A = \begin{pmatrix} a_1 & b_1 \\ (D-1)b_1/4 & a_1 + b_1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} a_2 & b_2 \\ (D-1)b_2/4 & a_2 + b_2 \end{pmatrix}.$$

Certainly $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in S$, and we also have that

$$A - B = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ (D-1)(b_1 - b_2)/4 & (a_1 - a_2) + (b_1 - b_2) \end{pmatrix} \in S \quad \text{and}$$

$$AB = \begin{pmatrix} a_1a_2 + (D-1)b_1b_2/4 & a_1b_2 + b_1a_2 + b_1b_2 \\ (D-1)(a_1b_2 + a_2b_1 + b_1b_2)/4 & (a_1a_2 + (D+1)b_1b_2/4) + (a_1b_2 + a_2b_1 + b_1b_2) \end{pmatrix} \in S,$$

and therefore S is a subring of $M_2(\mathbb{Z})$ as desired.

Consider now a map $\phi : \mathcal{O} \to S$ defined as $a + b\delta \mapsto \begin{pmatrix} a & b \\ Db & a+b \end{pmatrix}$. We aim to show that ϕ is a ring homomorphism. Certainly ϕ is well defined for the same reasons as in part (b). Then we have the following for arbitrary $a_1 + b_1\delta,\ a_2 + b_2\delta \in \mathcal{O}$:

$$\begin{aligned}
\phi((a_1 + b_1\delta) + (a_2 + b_2\delta)) &= \phi((a_1 + a_2) + (b_1 + b_2)\delta) \\
&= \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ (D-1)(b_1+b_2)/4 & a_1 + a_2 + b_1 + b_2 \end{pmatrix} \\
&= \begin{pmatrix} a_1 & b_1 \\ (D-1)b_1/4 & a_1 + b_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ (D-1)b_2/4 & a_2 + b_2 \end{pmatrix} \\
&= \phi(a_1 + b_1\delta) + \phi(a_2 + b_2\delta), \\
\phi((a_1 + b_1\delta)(a_2 + b_2\delta)) &= \phi((a_1a_2 + b_1b_2(D-1)/4) + (a_1b_2 + a_2b_1 + b_1b_2)\delta) \\
&= \begin{pmatrix} a_1a_2 + b_1b_2(D-1)/4 & a_1b_2 + a_2b_1 + b_1b_2 \\ (D-1)(a_1b_2 + a_2b_1 + b_1b_2)/4 & (a_1a_2 + (D-1)b_1b_2/4) + (a_1b_2 + a_2b_1 + b_1b_2) \end{pmatrix} \\
&= \begin{pmatrix} a_1 & b_1 \\ (D-1)b_1/4 & a_1 + b_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ (D-1)b_2/4 & a_2 + b_2 \end{pmatrix} \\
&= \phi(a_1 + b_1\delta)\phi(a_2 + b_2\delta).
\end{aligned}$$

Indeed, we see that ϕ is a ring homomorphism. We apply the same reasoning as in part (b) to give that in fact ϕ is a ring isomorphism. □

17 Let R and S be nonzero rings with identity and denote their respective identities by 1_R and 1_S. Let $\phi : R \to S$ be a nonzero homomorphism of rings.

(a) Prove that if $\phi(1_R) \neq 1_S$, then $\phi(1_R)$ is a zero divisor in S. Deduce that if S is an integral domain, then every ring homomorphism $R \to S$ sends $1_R \mapsto 1_S$.

Proof. Denote $\phi(1_R) = a$ where $a \neq 1$. If $a = 0$ then $\phi(x) = \phi(1_R x) = \phi(1_R)\phi(x) = 0 \cdot \phi(x) = 0$. Then we have that $\phi = 0$ which is a contradiction. So $a \neq 0$. Also, we have $a = \phi(1_R) = \phi(1_R 1_R) = \phi(1_R)\phi(1_R) = a^2$, and therefore $a = a^2$, which we rewrite as $a(a-1) = (1-a)a = 0$, and we see that indeed a is a zero divisor. If S is an integral domain then we have a contradiction, so if $\phi : R \to S$ is a nonzero ring homomorphism between unital rings R, S, then $1_R \mapsto 1_S$. □

(b) Prove that if $\phi(1_R) = 1_S$, then $\phi(u)$ is a unit in S and that $\phi(u^{-1}) = \phi(u)^{-1}$ for each unit u of R.

Proof. Let $u \in R$ be a unit. Then

$$\phi(u)\phi(u^{-1}) = \phi(uu^{-1}) = \phi(1_R) = 1_S = \phi(1_R) = \phi(u^{-1}u) = \phi(u^{-1})\phi(u).$$

So $\phi(u)$ is a unit, and $\phi(u^{-1}) = \phi(u)^{-1}$ follows from the uniqueness of inverses. □

Section 7.4

30 Let I be an ideal of the commutative ring R and define rad $I = \{r \in R : r^n \in I \text{ for some } n \in \mathbb{Z}^+\}$ called the *radical* of I. Prove that rad I is an ideal containing I and that (rad I)$/I$ is the nilradical of the quotient ring R/I, that is (rad I)$/I = \mathfrak{N}(R/I)$ (cf. §7.3 Ex. 29).

Proof. First notice that $I \subset$ rad I as $a \in I$ implies $a^1 \in I$. So, rad $I \neq \emptyset$. Take $a, b \in$ rad I where $a^n, b_m \in I$. Then we have

$$(a+b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i b^{m+n-i} \text{ via Exercise 7.3.25.}$$

If $i \geq n$ then $a^i \in I$ and if $i < n$ then $b^{m+n-i} \in I$ as I is an ideal. So every term in $(a+b)^{m+n}$ is in I, so $(a+b)^{m+n} \in I$. Also $(ra)^n = r^n a^n \in I$, in particular $(-a)^n \in R$ for arbitrary $r \in R$. So rad $I \trianglelefteq R$.

Next, we have the following bidirectional implications:

$$\begin{aligned} x + I \in (\text{rad } I)/I &\iff x \in \text{rad } I \\ &\iff x^n \in I \text{ for } n \geq 1 \\ &\iff x^n + I = 0 \text{ in } R/I \text{ for } n \geq 1 \\ &\iff (x+I)^n = 0 \text{ in } R/I \text{ for } n \geq 1 \\ &\iff x + I \in \mathfrak{N}(R/I). \end{aligned}$$

Therefore (rad $I)/I = \mathfrak{N}(R/I)$. □

37 A commutative ring R is called a *local ring* if it has a maximal ideal. Prove that if R is a local ring with maximal ideal M then every element of $R \setminus M$ is a unit. Prove conversely that if R is a commutative ring with 1 in which the set of nonunits forms an ideal M, then R is a local ring with unique maximal ideal M.

Proof. Consider some $x \in R \setminus M$ for the sake of contradiction. If it is not a unit, then it is contained in a maximal ideal. However, since local rings have a unique maximal ideal, x being not a unit would place x in M $\Rightarrow\Leftarrow$

Suppose for the second part that M is an arbitrary maximal ideal of R. Then certainly $M \trianglelefteq R$ is proper by definition. Also consider the ideal N generated by non unit elements of R. Since $1 \in R$ is a unit, we have that $N \trianglelefteq R$ is proper. So, since M has all elements which are non units, we must have $M \subset N$. But since M is maximal, we must have that $M = N$. So indeed N is the unique maximal ideal of R, which must be a local ring. □

Section 8.1

9 Prove that the ring of integers $\mathcal{O}$ in the quadratic integer ring $\mathbb{Q}(\sqrt{2})$ is a Euclidean Domain with respect to the norm given by the absolute value of the field norm N in §7.1.

Proof. Note first that $\mathcal{O}$ is an integral domain. Consider the following norm: for an element $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, we have $N(a + b\sqrt{2}) = |a^2 - 2b^2|$. Then $M : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}_+$ is a norm on $\mathbb{Z}[\sqrt{2}]$. We aim to show that a division algorithm exists. Define elements $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$ to be arbitrary elements of $\mathbb{Z}[\sqrt{2}]$. Then we have the following:

$$\frac{x}{y} = \frac{(ac - 2bd) + (bc - ad)\sqrt{2}}{c^2 - 2d^2} =: r + s\sqrt{2}.$$

Take n to be the integer closest to $r \in \mathbb{Q}$ and let m be the integer closest to $s \in \mathbb{Q}$, then $|r - n| \leq 1/2$ and $|s - m| \leq 1/2$. Define now $t := r - n + (s - m)\sqrt{2}$. Then

$$t = r + s\sqrt{2} - (n + m\sqrt{2}) = \frac{x}{y} - (n + m\sqrt{2}).$$

Then we have that $yt = x - (n + m\sqrt{2})y \in \mathbb{Z}[\sqrt{2}]$. Therefore we have that $x = (n + m\sqrt{2})y + yt$ where $(n + m\sqrt{2}), yt \in \mathbb{Z}[\sqrt{2}]$. Then we have the following norm estimate:

$$N(t) = |(r-n)^2 - 2(s-m)^2| \leq |r-n|^2 + 2|s-m|^2 \leq \frac{1}{4} + 2\frac{1}{4} = \frac{3}{4}.$$

Since N is multiplicative, we have that $N(yt) = N(y)N(t) \leq \frac{3}{4}N(y) < N(y)$. So, $x = (n + m\sqrt{2})y + yt$ gives a suitable division algorithm, and $\mathcal{O}$ is a Euclidean Domain as desired. □