1 Exercise 1: Not-quite-all-rationals

1.1 Problem

Fix an integer \(m\). An \(m\)-integer shall mean a rational number \(r\) such that there exists a \(k \in \mathbb{N}\) satisfying \(m^k r \in \mathbb{Z}\).

For example:

- Each integer \(r\) is an \(m\)-integer (since \(m^0 r \in \mathbb{Z}\) for \(k = 0\)).

- The rational number \(\frac{5}{12}\) is a 6-integer (since \(6^k \cdot \frac{5}{12} \in \mathbb{Z}\) for \(k = 2\)), but neither a 2-integer nor a 3-integer (since multiplying it by a power of 2 will not “get rid of” the prime factor 3 in the denominator, and vice versa\(^2\)).

- The 1-integers are the integers (since \(1^k r = r\) for all \(r\)).

- Every rational number \(r\) is a 0-integer (since \(0^k r \in \mathbb{Z}\) for \(k = 1\)).

\(^1\)You don’t need to prove these.

\(^2\)You would have to be more rigorous than this in your solution, if you were to make an argument like this.
Let $R_m$ denote the set of all $m$-integers. Prove the following:

(a) The set $R_m$ (endowed with the usual addition, the usual multiplication, the usual integer 0 as zero, and the usual integer 1 as unity) is a commutative ring.
   (You don’t need to prove axioms like commutativity of multiplication, since these follow from the corresponding facts about rational numbers, which are well-known. You only need to check that $R_m$ is closed under addition and multiplication and contains additive inverses of all its elements.)

(b) Let $x \in \mathbb{Q}$ be nonzero. Then, $x \in R_m$ if and only if every prime $p$ satisfying $w_p(x) < 0$ satisfies $p | m$. Here, we are using the notation $w_p(r)$ defined in Exercise 3.4.1 of the class notes.

1.2 Remark

The ring $R_m$ is an example of a ring “between $\mathbb{Z}$ and $\mathbb{Q}$”. Note that $R_1 = \mathbb{Z}$ and $R_0 = \mathbb{Q}$, whereas $R_2 = R_4 = R_8 = \cdots$ is the ring of all rational numbers that can be written in the form $a/2^k$ with $a \in \mathbb{Z}$ and $k \in \mathbb{N}$.

1.3 Solution

[...]

2 Exercise 2: Rings with $x^2 = x$

2.1 Problem

Let $K$ be a ring with the property that

$$u^2 = u \quad \text{for all } u \in K. \quad (1)$$

(Examples of such rings are $\mathbb{Z}/2$ as well as the “power set” ring $(\mathcal{P}(S), \triangle, \cap, \emptyset, S)$ constructed from any given set $S$.)

Prove the following:

(a) We have $2x = 0$ for each $x \in K$.

(b) We have $-x = x$ for each $x \in K$.

(c) We have $xy = yx$ for all $x, y \in K$. (In other words, the ring $K$ is commutative.)

(As usual, “0” stands for the zero of the ring $K$.)

[Hint: For part (a), apply (1) to $u = x$ but also to $u = 2x = x + x$, and see what comes out. For part (c), apply (1) to $u = x + y$.]

This means that every $a, b \in R_m$ satisfy $a + b \in R_m$ and $ab \in R_m$. 
2.2 Remark

You might wonder what happens if we replace (1) by

$$u^3 = u \quad \text{for all } u \in \mathbb{K}. \quad (2)$$

This no longer leads to $2x = 0$ (nor to $3x = 0$ as you might perhaps expect). Instead, it can be shown that $6x = 0$ for all $x \in \mathbb{K}$. It can also be shown that it leads to $xy = yx$.

2.3 Solution

[...]

3 Exercise 3: A matrix of gcds

3.1 Problem

In this exercise, we shall again use the Iverson bracket notation:

Let $n \in \mathbb{N}$. Let $G$ be the $n \times n$-matrix

$$(\gcd (i, j))_{1 \leq i, j \leq n} = \begin{pmatrix}
gcd (1, 1) & \gcd (1, 2) & \cdots & \gcd (1, n) \\
gcd (2, 1) & \gcd (2, 2) & \cdots & \gcd (2, n) \\
\vdots & \vdots & \ddots & \vdots \\
gcd (n, 1) & \gcd (n, 2) & \cdots & \gcd (n, n)
\end{pmatrix}.$$

Let $L$ be the $n \times n$-matrix

$$([j \mid i])_{1 \leq i, j \leq n} = \begin{pmatrix}[1 \mid 1] & [2 \mid 1] & \cdots & [n \mid 1] \\
[1 \mid 2] & [2 \mid 2] & \cdots & [n \mid 2] \\
\vdots & \vdots & \ddots & \vdots \\
[1 \mid n] & [2 \mid n] & \cdots & [n \mid n]
\end{pmatrix}.$$

Let $D$ be the $n \times n$-matrix

$$([i = j] \phi (i))_{1 \leq i, j \leq n} = \begin{pmatrix}\phi (1) & 0 & 0 & \cdots & 0 \\
0 & \phi (2) & 0 & \cdots & 0 \\
0 & 0 & \phi (3) & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & \phi (n)
\end{pmatrix}.$$

Prove that $G = LDL^T$.

[Hint: Diagonal matrices are particularly easy to multiply with other matrices. For example, given a diagonal matrix $D = ([i = j] d_i)_{1 \leq i, j \leq n}$ (where $d_1, d_2, \ldots, d_n$ are $n$ elements of a ring $\mathbb{K}$) and an arbitrary matrix $A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq m}$ (over the same ring $\mathbb{K}$), the product $DA$ is simply given by

$$DA = (d_i a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq m}.$$\footnote{We are using the standard notation $A^T$ for the transpose of a matrix $A$. This transpose is defined as follows: If $A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq m}$, then $A^T = (a_{j,i})_{1 \leq i \leq m, 1 \leq j \leq n}$.}]

Darij Grinberg, 00000000 3 dgrinber@umn.edu
(That is, multiplying by a diagonal matrix on the left is tantamount to rescaling each row by the corresponding entry of the diagonal matrix.) You can use the formula [3] without proof (though its easy proof is instructive).

3.2 Remark

As the names suggest, the matrix $L$ is lower-triangular (so that the matrix $L^T$ is upper-triangular), and the matrix $D$ is diagonal. Thus, $G = LDL^T$ is an instance of an $LDU$ decomposition.

3.3 Solution

[...]

4 Exercise 4: Idempotent and involutive elements

4.1 Problem

Let $\mathbb{K}$ be a ring.

An element $a$ of $\mathbb{K}$ is said to be idempotent if it satisfies $a^2 = a$.

An element $a$ of $\mathbb{K}$ is said to be involutive if it satisfies $a^2 = 1$.

(a) Let $a \in \mathbb{K}$. Prove that if $a$ is idempotent, then $1 - 2a$ is involutive.

(b) Now, assume that 2 is cancellable in $\mathbb{K}$; this means that if $u$ and $v$ are two elements of $\mathbb{K}$ satisfying $2u = 2v$, then $u = v$. Prove that the converse of the claim of part (a) holds: If $a \in \mathbb{K}$ is such that $1 - 2a$ is involutive, then $a$ is idempotent.

(c) Now, let $\mathbb{K} = \mathbb{Z}/4$. Find an element $a \in \mathbb{K}$ such that $1 - 2a$ is involutive, but $a$ is not idempotent.

4.2 Remark

The idempotent elements of $\mathbb{R}$ are 0 and 1. The involutive elements of $\mathbb{R}$ are 1 and $-1$. A matrix ring like $\mathbb{R}^{n \times n}$ usually has infinitely many idempotent elements (viz., all projection matrices on subspaces of $\mathbb{R}^n$) and infinitely many involutive elements (viz., all matrices $A$ satisfying $A^2 = I_n$; for instance, all reflections across hyperplanes are represented by such matrices).

Part (a) of this exercise assigns an involutive element to each idempotent element of $\mathbb{K}$. If 2 is invertible in $\mathbb{K}$ (that is, if the element $2 \cdot 1_\mathbb{K}$ has a multiplicative inverse), then this assignment is a bijection (as can be easily derived from (a)). Part (c) shows that we cannot drop the “2 is cancellable” condition in part (b).

4.3 Solution

[...]

Darij Grinberg, 00000000
dgrinber@umn.edu
5 Exercise 5: The matrix approach to Fibonacci numbers

5.1 Problem

Let $A$ be the $2 \times 2$-matrix $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ over $\mathbb{Z}$. Consider also the identity matrix $I_2$.

Let $F$ be the subset 
\[ \{aA + bI_2 \mid a, b \in \mathbb{Z}\} = \left\{ \begin{pmatrix} b & a \\ a & a + b \end{pmatrix} \mid a, b \in \mathbb{Z} \right\} \]

of the matrix ring $\mathbb{Z}^{2 \times 2}$.

(a) Prove that $A^2 = A + I_2$.

(b) Prove that the set $F$ (equipped with the addition of matrices, the multiplication of matrices, the zero $0_{2 \times 2}$ and the unity $I_2$) is a commutative ring.

(Again, you don’t need to check the ring axioms, as we already know that they hold for arbitrary matrices and thus all the more for matrices in $F$. But you do need to check commutativity of multiplication in $F$, since it does not hold for arbitrary matrices. You also need to check that $F$ is closed under addition and multiplication and has additive inverses.)

Let $(f_0, f_1, f_2, \ldots)$ be the Fibonacci sequence (which we have already encountered on homework set #5). Recall that it is defined recursively by

\[ f_0 = 0, \quad f_1 = 1, \quad \text{and} \quad f_n = f_{n-1} + f_{n-2} \text{ for all } n \geq 2. \]

(c) Prove that $A^n = f_n A + f_{n-1} I_2$ for all positive integers $n$.

(d) Prove that $f_{n+m} = f_n f_{m+1} + f_{n-1} f_m$ for all positive integers $n$ and all $m \in \mathbb{N}$.

Now, define a further matrix $B \in F$ by $B = (-1) A + 1 I_2 = I_2 - A$.

(e) Prove that $B^2 = B + I_2$ and $B^n = f_n B + f_{n-1} I_2$ for all positive integers $n$.

(f) Prove that $A^n - B^n = f_n (A - B)$ for all $n \in \mathbb{N}$.

(g) Prove (again!) that $f_d \mid f_{dn}$ for any nonnegative integers $d$ and $n$.

[Hint: One way to prove (d) is by comparing the $(1, 1)$-th entries of the two (equal) matrices $A^n A^{m+1}$ and $A^{n+m+1}$, after first using part (c) to expand these matrices.

For part (g), compare the $(1, 1)$-th entries of the matrices $A^d - B^d$ and $A^{dn} - B^{dn}$, after first proving that $A^d - B^d \mid A^{dn} - B^{dn}$ in the commutative ring $F$. Note that divisibility is a tricky concept in general rings, but $F$ is a commutative ring, which lets many arguments from the integer setting go through unchanged.]

5.2 Remark

Contrast the ring $F$ with the ring $\mathbb{Z}[d]$ from Exercise 5 on homework set #5. Both of these rings, as we see, can be used to prove that $f_d \mid f_{dn}$ for any nonnegative integers $d$ and $n$. What else do these rings have in common?
5.3 Solution

[...]

6 Exercise 6: ISBNs vs. fat fingers

6.1 Problem

An ISBN shall mean a 10-tuple \((a_1, a_2, \ldots, a_{10}) \in \{0, 1, \ldots, 10\}^{10}\) such that

\[1a_1 + 2a_2 + \cdots + 10a_{10} \equiv 0 \pmod{11}.\]

(For example, the 10-tuple \((1, 1, \ldots, 1)\) is an ISBN.)

Prove the following:

(a) If \(a = (a_1, a_2, \ldots, a_{10})\) and \(b = (b_1, b_2, \ldots, b_{10})\) are two ISBNs that are equal in all but one entry (i.e., there exists some \(k \in \{1, 2, \ldots, 10\}\) such that \(a_i = b_i\) for all \(i \neq k\), then \(a = b\).

(b) If an ISBN \(a = (a_1, a_2, \ldots, a_{10})\) is obtained from an ISBN \(b = (b_1, b_2, \ldots, b_{10})\) by swapping two entries (i.e., there exist \(k, \ell \in \{1, 2, \ldots, 10\}\) such that \(a_k = b_\ell\) and \(a_\ell = b_k\) and \(a_i = b_i\) for all \(i \notin \{k, \ell\}\)), then \(a = b\).

6.2 Remark

What we called ISBN here is essentially the definition of an ISBN-10 – an international standard for book identifiers used from the 1970s until 2007. For example, the ISBN-10 of the Graham/Knuth/Patashnik book “Concrete Mathematics” is “0-201-55802-5”, which corresponds to \((0, 2, 0, 1, 5, 5, 8, 0, 2, 5)\); you can check that this is indeed an ISBN according to our definition.

(An “X” in a real-life ISBN stands for an entry that is 10.)

As this exercise shows, ISBNs have an error-detection property: If you make a typo in a single digit or accidentally swap two digits, the result will not be an ISBN, so you will know that something has gone wrong. This helps you avoid ordering the wrong book from a bookstore or library. Credit card numbers have a similar error-detection feature.

This is one of the simplest examples of an error correction code. We may or may not see more of them in class. For now, you can think about how to define “ISBNs”

- in \(\{0, 1, \ldots, 4\}^4\);
- in \(\{0, 1, \ldots, 6\}^6\);
- in \(\{0, 1, \ldots, 8\}^8\) (this is harder!).

6.3 Solution

[...]

References

Darij Grinberg, 00000000
dgrinber@umn.edu