

Homework 1

Joshua Cragun *

August 2018

*Prof. Savin, Math 3210

Question 1

For $i = 0, \dots, 10$, construct the greatest rational number in the cut of the square root of 3 in the form of a (non reduced) fraction $a_i = \frac{x_i}{2^i}$, and the least rational number not in the cut in the same form, $b_i = \frac{y_i}{2^i}$.

Solution:

To be begin, we shall start with a_0 and b_0 . Recall the definition of a cut bounded by $\sqrt{3}$.

$$(\sqrt{3})^* := \{r \in \mathbb{Q}^+ \mid r^2 < 3\}$$

This will make it quite easy to determine which rational numbers are in and not in $(\sqrt{3})^*$. From the definition of a_0 and b_0 , it is clear that they will be integers (specifically, the two closest integers above and below $\sqrt{3}$) since the denominator is simply 2^0 , or one.

Let us then describe an algorithm for defining what the next a_i and b_i will be. We know that there exists an integer n such that $(\frac{n}{m})^2 < 3$ and $(\frac{n+1}{m})^2 > 3$ where $m \in \mathbb{N}$ as a consequence of the Archimedean Principle. Because the binary operation of averaging two numbers naturally multiplies the denominator by 2 and finds the midpoint between two bounds (which will be tending towards $\sqrt{3}$), it is optimal for producing the following the following a_i and b_i in the series.

A “brute force” recurrence relation will then be described as follows:

1. Define possible greatest/smallest rational number in/out of the cut of a given denominator $m \in \mathbb{N}$ as $c_i = \frac{n}{m}$ as the average of a_{i-1} and b_{i-1} with $c_0 = \frac{0}{1}$
2. If $n^2 < 3 \cdot m^2$ increment n by one until $n^2 > 3 \cdot m^2$, then $\frac{n}{m} = b_i$ and $\frac{n-1}{m} = a_i$
3. Otherwise $n^2 > 3 \cdot m^2$, then decrement n by one until $n^2 < 3 \cdot m^2$, then $\frac{n}{m} = a_i$ and $\frac{n+1}{m} = b_i$

Given the exponential nature of how the denominator will change throughout the procedure, it could prove a tedious problem by hand, however computers can execute this algorithm very swiftly. But, for demonstrative purposes, I shall show how this algorithm finds a_0 and b_0 .

Start with $c_0 = \frac{0}{1}$. Then $c_0^2 = 0 < 3$, so increment the numerator by 1 until $c_0^2 > 3$, which happens after two increments ($c_0 = \frac{2}{1}$) as $c_0^2 = 2^2 = 4 > 3$.

Then we have:

$$\begin{aligned} a_0 &= \frac{n-1}{m} = \frac{2-1}{1} = 1 \\ b_0 &= c_0 = 2 \end{aligned} \tag{1}$$

Continuing this process for $i = 1, 2, \dots, 10$ we get:

1. $a_1 = \frac{3}{2}, b_1 = \frac{4}{2}$
2. $a_2 = \frac{6}{4}, b_2 = \frac{7}{4}$
3. $a_3 = \frac{13}{8}, b_3 = \frac{14}{8}$
4. $a_4 = \frac{27}{16}, b_4 = \frac{28}{16}$
5. $a_5 = \frac{55}{32}, b_5 = \frac{56}{32}$
6. $a_6 = \frac{110}{64}, b_6 = \frac{111}{64}$
7. $a_7 = \frac{221}{128}, b_7 = \frac{222}{128}$
8. $a_8 = \frac{443}{256}, b_8 = \frac{444}{256}$
9. $a_9 = \frac{886}{512}, b_9 = \frac{887}{512}$
10. $a_{10} = \frac{1773}{1024}, b_{10} = \frac{1774}{1024}$

Question 2

Let α and β be two cuts of \mathbb{Q}^+ . Let $\alpha \cdot \beta = \{rs \mid r \in \alpha, s \in \beta\}$. Prove that $\alpha \cdot \beta$ is a cut of \mathbb{Q}^+ .

Proof. To show that any given set is a cut, one must show that for a given set S :

1. $\forall x \in S$, if $y < x$, then $y \in S$.
 2. S has no maximal element.
- 1.** Let $c = a \cdot b \in \alpha \cdot \beta$ where $a \in \alpha$ and $b \in \beta$ and α and β are cuts of \mathbb{Q}^+ . Let $d < c$. Thus $d < a \cdot b$. Then $\frac{d}{b} < a$ (the inequality will not flip since this is over \mathbb{Q}^+). Since α defines a cut and $\frac{d}{b} < a$, $\frac{d}{b} \in \alpha$. Then $d = \frac{d}{b} \cdot b$ where $\frac{d}{b} \in \alpha, b \in \beta$, so $d \in \alpha \cdot \beta$.
- 2.** Let $c = a \cdot b \in \alpha \cdot \beta$. Since α is a cut, $\exists a_2 \in \alpha : a_2 > a$, which then means $a_2 \cdot b \in \alpha \cdot \beta$ and $a_2 \cdot b > a \cdot b = c$. Thus, for any element of $\alpha \cdot \beta$, one can find an element that is larger than it, i.e. it has no maximal element.

And since properties 1 and 2 have been shown, $\alpha \cdot \beta$ must be a Dedekind cut. \square

Question 3

Let $1^* = \{r \in \mathbb{Q}^+ \mid r < 1\}$. Prove that $\alpha \cdot 1^* = \alpha$ for any cut of \mathbb{Q}^+ .

Proof. Take any $a \cdot b \in \alpha \cdot 1^*$, where $a \in \alpha$ and $b \in 1^*$. Then by definition, $b < 1$. Then we have $a \cdot b < a \cdot 1 = a$, and therefore since α defines a Dedekind cut, $a \cdot b \in \alpha$. So then any member of $\alpha \cdot 1^*$ must also be a member of α , thus $\alpha \cdot 1^* \subseteq \alpha$.

Conversely, take any member $a \in \alpha$. Because α is a Dedekind cut, there is an $a_2 \in \alpha : a_2 > a$. Then we have $a = a_2 \cdot \frac{a}{a_2}$ where $\frac{a}{a_2} < 1$ since $a < a_2$, which means that $\frac{a}{a_2} \in 1^*$; hence from the definition of $\alpha \cdot 1^*$, any member of α is also a member of $\alpha \cdot 1^*$, i.e. $\alpha \subseteq \alpha \cdot 1^*$.

Thus, $\alpha \cdot 1^* = \alpha$.

□

Question 4

Let α be a cut of \mathbb{Q}^+ . Construct a β such that $\alpha \cdot \beta = 1^*$.

Solution:

First we must hypothesize what such a set β could be. I have defined mine as follows:

$$\beta := \bigcup_{r \notin \alpha} (r^{-1})^*$$

Where r denotes a rationally bounded cut. In other words, β is the union of all rationally bounded cuts not contained in the given set α with their upper bounds inverted. (e.g. If α is 2^* , since 3^* is not a subset of that cut, $\frac{1}{3}^*$ is in the union that defines the inverse of the cut of 2, as well as $\frac{2}{5}^*$, and $\frac{100}{201}^*$, and so on.) Note that every set in the union has rational bounds, but due to the dense nature of rational numbers, the elements of an irrationally bounded cut will be contained in an adjacent rationally bounded cut. Further, the set is bounded above and has a supremum; namely, it is the inverse of the infimum of $\neg\alpha$. $\text{Sup}(\beta) \notin \beta$ since the highest cut in the union would be the cut *bounded* by the inverse of $\text{Inf}(\neg\alpha)$. We must now show that β is a cut.

Proof. Let $b \in \beta$ and $c < b$. Because β is a union of cuts, there must be some cut $\beta_0 \subseteq \beta$ that b is a member of. Then, since $c < b$ and $b \in \beta_0$, $c \in \beta_0 \subseteq \beta$. So then $c \in \beta$.

Next, Take any $b \in \beta$. Because β is a union of cuts, there must be some cut $\beta_0 \subseteq \beta$ that b is a member of. Because β_0 is a cut, there must be some $b_2 \in \beta_0 : b_2 > b$, since it has no maximal element. Then, since $b_2 \in \beta_0 \subseteq \beta$, $b_2 \in \beta$. Thus, for any element in β , one can find another element of β that is larger. Thus β has no maximal element.

Hence β is a cut. □

Now it must be shown that $\alpha \cdot \beta = 1^*$.

Proof. First one must show that $\alpha \cdot \beta \subseteq 1^*$.

Take any $a \cdot b \in \alpha \cdot \beta$, $a \in \alpha$, $b \in \beta$. By definition, $b < \frac{1}{r}$ where r is $\text{Inf}(\neg\alpha)$. Then $a < \text{Sup}(\alpha) \leq r < \frac{1}{b}$. Then $a \cdot b < \frac{a}{r}$. Because $a, r \in \mathbb{Q}^+$ and $a < r$, $a \cdot b < \frac{a}{r} < 1$ which from the definition of 1^* means that $a \cdot b \in 1^*$. Thus, $\alpha \cdot \beta \subseteq 1^*$.

Next it will be shown that $1^* \subseteq \alpha \cdot \beta$.

Take any $p \in 1^*$, so $0 < p < 1$. Then the following is true:

$$p < 1 - \frac{1}{m+1} = \frac{m}{m+1}$$

Where $m \in \mathbb{N}$ is greater then or equal to some boundary $n \in \mathbb{N}$ (i.e. n is the smallest value that satisfies the given inequality).

Take any $a \in \alpha$. Then define some $q \in \mathbb{Q}^+$ such that $0 < q < \frac{a}{n}$. Then there exists an $m \geq n$ such that $mq \in \alpha$, but $(m+1)q \notin \alpha$. So then we have:

$$\frac{p}{mq} < \frac{m}{m+1} \cdot \frac{1}{mq} = \frac{1}{(m+1)q}$$

Because $(m+1)q \notin \alpha$, $(\frac{1}{(m+1)q})^* \subset \beta$. Since $\frac{p}{mq} < \frac{1}{(m+1)q}$, we know that $\frac{p}{mq} \in (\frac{1}{(m+1)q})^*$. So then $\frac{p}{mq} \in \beta$.

Hence, $p = mq \cdot \frac{p}{mq} \in 1^*$ where $mq \in \alpha$ and $\frac{p}{mq} \in \beta$.

Thus any members of 1^* can be expressed as a product of members of α and β . So then $1^* \subseteq \alpha \cdot \beta$ and thus $\alpha \cdot \beta = 1^*$.

□

Question 5

Let \mathbb{C} be the set of 2×2 matrices in the form

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

Where a and b are real numbers.

Part 1: If $A, B \in \mathbb{C}$, prove that $A + B$, $A - B$, and AB are in \mathbb{C} and that $AB = BA$.

Proof. If we have $A = (a, b)$ and $B = (c, d)$, then $A + B =$

$$\begin{pmatrix} a + c & -(b + d) \\ b + d & a + c \end{pmatrix}$$

Since it maintains the described form for \mathbb{C} , $A + B \in \mathbb{C}$. Similarly $A - B =$

$$\begin{pmatrix} a - c & -(b - d) \\ b - d & a - c \end{pmatrix}$$

Which likewise maintains the criteria to be considered a member of \mathbb{C} since it matches the desired form and the sums and differences in each matrix entry are also real. Similarly, $AB =$

$$\begin{pmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{pmatrix}$$

Which is clearly also a meets the criteria to be considered a member of \mathbb{C} . Consider BA .

$$\begin{pmatrix} ca - db & -(cb + da) \\ cb + da & ca - db \end{pmatrix}$$

Which, since the real multiplication and addition binary operations are commutative, it is equivalent to AB . \square

This implies that \mathbb{C} forms a ring since the rest of a ring's properties are already innate to matrices as a whole and their operations (e.g. the

multiplication of matrices is already known to be associative, and a zero and identity matrix have already been established, for instance.)

Part 2: For every non-zero $A \in \mathbb{C}$, find $B \in \mathbb{C}$ such that $AB = 1$.

Let A be of the same form as it was in part 1. It is known that a 2×2 matrix X is invertable if $\text{Det}(X) \neq 0$. Let us consider $\text{Det}(A)$.

$$\text{Det}(A) = (a \cdot a) - (-b \cdot b) = a^2 + b^2$$

Thus, the only way the determinate of $A = 0$ is if a and b are zero. But since this is over all non-zero matrices, we can see then that all nonzero elements of \mathbb{C} are invertable. Let us then characterize the inverse of A . As per tradition, the inverse of 2×2 matrix is like so:

$$A^{-1} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}^{-1} = \frac{1}{a^2 + b^2} \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

Part 3: Consider \mathbb{C}' , the set of all 2×2 matrices in the forms

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

Where $a, b \in \mathbb{R}$. What fails when verifying if \mathbb{C}' qualifies as a field?

What fails is invertability. Consider the determinant of the matrix above (call it A):

$$\text{Det}(A) = (a \cdot a) - (b \cdot b) = a^2 - b^2$$

One sees the problem with this as soon as they consider when $a^2 - b^2 = 0$ which is satisfied by $a = \pm b$. Thus, there are nonzero elements of \mathbb{C}' that are not invertable. Thus, \mathbb{C}' cannot be a field.