MTH 4104 Mock Exam Paper (2023-2024)

Shu SASAKI

This mock paper is purposely slightly harder (but only just) than the actual paper I've written this academic year.

Q1. Let $\mathcal{R}$ be a relation on the set of positive integers:

$$a\mathcal{R}b \Leftrightarrow \text{either } a \text{ divides } b\text{, or } b \text{ divides } a$$

Is this an equivalence relation? If so prove it. If not, explain exactly which axioms it fails to satisfy, by giving an explicit counter-example for each.

A1. • $a\mathcal{R}a$ holds since a always divides a.

• If $a\mathcal{R}b$ holds, then $b\mathcal{R}a$ holds. This follows by definition.

• If $a\mathcal{R}b$ and $b\mathcal{R}c$, should $a\mathcal{R}c$ hold? Not necessarily. For example, $2\mathcal{R}6$ and $6\mathcal{R}3$ hold; but $2\mathcal{R}3$ does not hold (as neither 2 divides 3 nor 3 divides 2). Hence $\mathcal{R}$ is NOT an equivalence relation (failing on the transitivity).

Q2. Solve the following set of equations in X and Y in $\mathbb{F}_{13}$:

$$\begin{aligned} X + 4Y &\equiv 17 \mod 13 \\ X - 2Y &\equiv 6 \mod 13 \end{aligned}$$

A2. Subtracting the second congruence equation from the first, we get $6Y \equiv 11 \mod 13$. To solve this equation in Y, we use Euclid's algorithm to find a pair of integers a and b such that $6a + 13b = \gcd(6, 13) = 1$. Granted, multiplying $6Y \equiv 11$ by a, we get $6aY \equiv 11a$ which is $Y \equiv 11a \mod 13$ (because $6a = -13b + 1 \equiv 1 \mod 13$). By Euclid's algorithm or otherwise, we find $(a, b) = (11, -5)$ does the job. Therefore $Y \equiv 11 \cdot 11 = 121 \equiv 4 \mod 13$. Plugging this back into one of the given congruence equations, we find $X \equiv 1 \mod 13$. So $(X, Y) = (1, 4) \mod 13$ is the solution.

Q3. (1) Let G be the set of real numbers that are not equal to -1. Define a binary operation $*$ on G by

$$a * b = a + b + ab.$$

Prove that $(G, *)$ is a group.

(2)[Extra for Enthusiasts] Let S be a set consisting of four symbols $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$. Define a binary operation $*$ on S by the following table which describes (row) $*$ (column):

	♣	♢	♡	♠
♣	♣	♢	♡	♠
♢	♢	♡	♠	♣
♡	♡	♠	♣	♢
♠	♠	♣	♢	♡

Is $(S, *)$ a group? Justify your answer.

A3.(1) We check the group axioms.

(G0) Since $a+b+ab$ is evidently a real number, it remains to check it is not equal to -1 (if a and b are not). If $a+b+ab$ were equal to -1, then $a+b+ab+1=(a+1)(b+1)$ would be 0. However, since neither a nor b is equal to -1, this is a contradiction.

(G1) On one hand,

$$(a*b)*c=(a+b+ab)*c=(a+b+ab)+c+(a+b+ab)c=a+b+c+ab+bc+ca+abc.$$

On the other hand,

$$a*(b*c)=a*(b+c+bc)=a+(b+c+bc)+a(b+c+bc)=a+b+c+ab+bc+ca+abc.$$

Combining, $(a*b)*c=a*(b*c)$.

(G2) The identity element of G with respect to $*$ is 0. Indeed,

$$a*0=a+0+a0=a.$$

Similarly,

$$0*a=0+a+0a=a.$$

[How do we find e? We need to find e in G such that $a*e=a$, i.e. $a+e+ae=a$, for every a in G. Subtracting a from both sides of the equality, we get $e+ae=0$, i.e. $e(1+a)=0$. However, we know by assumption that a is not equal to -1 and as a result $1+a$ is never 0! The only way the product $e(1+a)$ attains 0 is that e itself is 0.]

(G3) The inverse of a is $-1+1/(1+a)$ (since $a\neq -1$, $1+a$ is non-zero). Indeed,

$$a*(-1+\frac{1}{1+a})=a+(-1)+\frac{1}{1+a}+a\left(-1+\frac{1}{(1+a)}\right)=a+(-1)+\frac{1}{1+a}-a+\frac{a}{1+a}=0.$$

Similarly, it is possible to verify $(-1+1/(1+a))*a=0$. [How do we find the inverse b of a in G? We need to find b such that $a*b=0$ (as seen in (G2), the identity is 0), i.e. $a+b+ab=0$. Adding 1 on both sides, we get $a+b+ab+1=1$, i.e. $(a+1)(b+1)=1$. Since $a\neq -1$, $1+a\neq 0$ and therefore $b+1=1/(1+a)$. In conclusion, $b=-1+1/(1+a)$]

(2) It is a group. (G0) Since all combinations of (row) $*$ (column) lie in S, (G0) holds (without further expenditure of effort). (G2) $\clubsuit$ is the identity element. Indeed, the first row and the first column prove (G2). (G3) According to the table, the inverse of $\clubsuit$ is $\clubsuit$ itself, the inverse of $\diamondsuit$ is $\spadesuit$, the inverse of $\heartsuit$ is $\heartsuit$ itself, and the inverse of $\spadesuit$ is $\diamondsuit$.
Parenthetically, it is easy to check from the 'symmetry' of the table with respect to the 'diagonals' that (G4) holds, hence $(S,*)$ is abelian. This is not part of Q3(2) though.

(G1) This is the hardest to check (formally). We can use the commutativity of $*$ to convince ourselves that it suffices to check (a quarter of) all possible combinations:

$$\clubsuit*(\clubsuit*\clubsuit)=\clubsuit*\clubsuit=(\clubsuit*\clubsuit)*\clubsuit$$

$$\clubsuit*(\clubsuit*\diamondsuit)=\clubsuit*\diamondsuit=(\clubsuit*\clubsuit)*\diamondsuit$$

$$\clubsuit*(\clubsuit*\heartsuit)=\clubsuit*\heartsuit=(\clubsuit*\clubsuit)*\heartsuit$$

$$\clubsuit * (\clubsuit * \spadesuit) = \clubsuit * \spadesuit = (\clubsuit * \clubsuit) * \spadesuit$$
$$\clubsuit * (\diamondsuit * \diamondsuit) = \clubsuit * \heartsuit = \heartsuit = \diamondsuit * \diamondsuit = (\clubsuit * \diamondsuit) * \diamondsuit$$
$$\clubsuit * (\diamondsuit * \heartsuit) = \clubsuit * \spadesuit = \spadesuit = \diamondsuit * \heartsuit = (\clubsuit * \diamondsuit) * \heartsuit$$
$$\clubsuit * (\diamondsuit * \spadesuit) = \clubsuit * \clubsuit = \clubsuit = \diamondsuit * \spadesuit = (\clubsuit * \diamondsuit) * \heartsuit$$
$$\clubsuit * (\heartsuit * \heartsuit) = \clubsuit * \clubsuit = \clubsuit = \heartsuit * \heartsuit = (\clubsuit * \heartsuit) * \heartsuit$$
$$\clubsuit * (\heartsuit * \spadesuit) = \clubsuit * \diamondsuit = \diamondsuit = \heartsuit * \spadesuit = (\clubsuit * \heartsuit) * \spadesuit$$
$$\clubsuit * (\spadesuit * \spadesuit) = \clubsuit * \heartsuit = \heartsuit = \spadesuit * \spadesuit = (\clubsuit * \spadesuit) * \spadesuit$$
$$\diamondsuit * (\diamondsuit * \diamondsuit) = \diamondsuit * \heartsuit = \heartsuit * \diamondsuit = (\diamondsuit * \diamondsuit) * \diamondsuit$$
$$\diamondsuit * (\diamondsuit * \heartsuit) = \diamondsuit * \spadesuit = \clubsuit = \heartsuit * \heartsuit = (\diamondsuit * \diamondsuit) * \heartsuit$$
$$\diamondsuit * (\diamondsuit * \spadesuit) = \diamondsuit * \clubsuit = \diamondsuit = \heartsuit * \spadesuit = (\diamondsuit * \diamondsuit) * \spadesuit$$
$$\heartsuit * (\heartsuit * \heartsuit) = \heartsuit * \clubsuit = \clubsuit * \heartsuit = (\heartsuit * \heartsuit) * \heartsuit$$
$$\heartsuit * (\heartsuit * \spadesuit) = \heartsuit * \diamondsuit = \spadesuit = \clubsuit * \spadesuit = (\heartsuit * \heartsuit) * \spadesuit$$
$$\spadesuit * (\spadesuit * \spadesuit) = \spadesuit * \heartsuit = \heartsuit * \spadesuit = (\spadesuit * \spadesuit) * \spadesuit$$

(I am sure no one goes down this road, but I feel morally obliged to show you how this is done!) or simply spot that the table seems to manifest the same set of additive relations as $S = \mathbb{Z}_4$ with $\clubsuit = [0]_4, \diamondsuit = [1]_4, \heartsuit = [2]_4$ and $\spadesuit = [3]_4$. In fact, I have used this viewpoint to pull off the calculations above. Since we know that $(\mathbb{Z}_4, +)$ is a group under addition, $(S, *)$ is a group.

Q4. Let $(R, +, \times)$ be a ring and 0 denote the identity element with respect to addition $+$. Prove that $a0 = 0a = 0$ for every element a in R.

A4. This is Proposition 16. By (R+2), $0+0 = 0$. Multiplying a from left, we obtain $a(0+0) = a0$. The LHS equals $a0+a0$ by (R×+), while the RHS equals $a0 = a0+0$ by (R+2) again. Plugging these back into the equality, we get

$$a0 + a0 = a0 + 0.$$

Proposition 15 on the other hand asserts $a + b = a + c$ implies $b = c$ for any a, b, c in R– this follows simply by subtracting the (unique) inverse of a from left

$$(-a)+a+b = (-a)+a+c \overset{(\text{R+1})}{\Rightarrow} (-a+a)+b = (-a+a)+c \overset{(\text{R+3})}{\Rightarrow} 0+b = 0+c \overset{(\text{R+2})}{\Rightarrow} b = c.$$

We therefore conclude that $a0 = 0$. On the other hand, multiplying a from right on $0 + 0 = 0$, we obtain $(0 + 0)a = 0a$ and therefore

$$0a + 0a = 0a + 0$$

as before. By Proposition 15 again, $0a = 0$.

Q5. Let $\mathbb{H}$ be Hamilton's quaternions, i.e. the set of elements of the form

$$c1 + c(p)p + c(q)q + c(r)r \in \mathbb{R}1 + \mathbb{R}p + \mathbb{R}q + \mathbb{R}r$$

where the basis elements $1, p, q$ and r satisfy the multiplicative relations

- $1p = p1 = p$, $1q = q1 = q$, $1r = r1 = r$,
- $p^2 = -1, q^2 = -1, r^2 = -1$,
- $pq = r, qp = -r$,
- $qr = p, rq = -p$,
- $rp = q, qr = -q$,

together with natural addition and multiplication (prescribed by the relation).

(1) What is the multiplicative inverse of $p+q-r$? (2) Is $\mathbb{H}$ a field? If so, prove it. If not, explain why.

A5. (1) In the lecture, we show that the multiplicative inverse of a non-zero element of $\mathbb{H}$ of the form $c + c(p)p + c(q)q + c(r)r$ is given by

$$\frac{c}{\mathcal{R}} - \frac{c(p)}{\mathcal{R}}p - \frac{c(q)}{\mathcal{R}}q - \frac{c(r)}{\mathcal{R}}r$$

where $\mathcal{R}$ is the positive real number $c^2 + c(p)^2 + c(q)^2 + c(r)^2$ (since the element is assumed to be non-zero, $c, c(p), c(q)$ and $c(r)$ are not simultaneously zero; and this translates as $\mathcal{R}$ being non-zero). The question asks the case when $(c, c(p), c(q), c(r)) = (0, 1, 1, -1)$. So the inverse we seek is

$$-\frac{1}{3}p - \frac{1}{3}q - \frac{-1}{3}r.$$

(2) $\mathbb{H}$ is not a field, because it is not commutative ring. For example, pq is not equal to qp.

Q6. Find polynomials $f(X)$ and $g(X)$ in $\mathbb{F}_3[X]$ such that $(X^8+[2])f(X)+([2]X^6+[2])g(X) = \gcd(X^8 + [2], [2]X^6 + [2])$ in $\mathbb{F}_3[X]$.

A6. Since $[2][2] = [4] = [1]$ in $\mathbb{F}_3 = \{[0], [1], [2]\}$, Euclid's algorithm in $\mathbb{F}_3[X]$ sees

$$\begin{aligned} X^8 + [2] &= [2]X^2([2]X^6 + [2]) + [2]X^2 + [2] \\ [2]X^6 + [2] &= (X^4 + [2]X^2 + [1])([2]X^2 + [2]) + [0]. \end{aligned}$$

Hence $[2]X^2 + [2]$ is a common divisor. To get the gcd, we need to find a monic polynomial of degree 2 that divides $[2]X^2 + [2]$ in $\mathbb{F}_3[X]$. To this end, it suffices to multiply $[2]X^2 + [2]$ by the multiplicative inverse of [2]. Since the inverse is [2] itself,

$$[2]([2]X^2 + [2]) = [4]X^2 + [4] = X^2 + [1].$$

The gcd is $X^2 + [1]$.

On the other hand, Euclid's algorithm shows

$$[2]X^2 + [2] = (X^8 + [2]) - [2]X^2([2]X^6 + [2]).$$

As we have did in finding gcd, to find f and g, we multiply this identity through by [2]. The LHS becomes $X^2 + [1]$ (as seen above), while the RHS should, correspondingly, become

$$[2](X^8 + [2]) - [4]X^2([2]X^6 + [2]) = [2](X^8 + [2]) - X^2([2]X^6 + [2]).$$

In other words, $(f,g) = ([2], -X^2)$ does the job.

Q7. Let σ be an element of S_{10} of the form

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 7 & 9 & 6 & 8 & 1 & 5 & 10 & 3 & 2 \end{pmatrix}$$

(1) Write σ in cycle notation . (2) Let τ be $(1)(2\,8\,6\,7)(3\,5\,4\,9)(10)$. Compute $\sigma \circ \tau^{-1}$ in cycle notatioon. (3) Determine the order of σ.

A7. (1) $(1\,4\,6)(2\,7\,5\,8\,10)(3\,9)$. (2) Since

$$\tau^{-1} = (1)(2\,7\,6\,8)(3\,9\,4\,5)(10) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 7 & 9 & 5 & 3 & 8 & 6 & 2 & 4 & 10 \end{pmatrix} =$$

$$\sigma \circ \tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 5 & 3 & 8 & 9 & 10 & 1 & 7 & 6 & 2 \end{pmatrix} = (1\,4\,8\,7)(2\,5\,9\,6\,10)(3).$$

(3) It is given by the lcm of the lengths of all cycles in the cycle expression of σ, i.e. $\mathrm{lcm}(3, 5, 2) = 30$.