Queen Mary
University of London

B. Sc. Examination by course unit 2014

MTH4104 Introduction to Algebra

Duration: 2 hours

Date and time: TBD

Model solutions

Question 1 (a) Give definitions of the terms (i) *relation*; [2]
(ii) *equivalence relation*. [3]

(b) Give an example of an equivalence relation on the set $\{1,2,3\}$ with exactly two equivalence classes. [3]

Solution (a) A *relation* on a set X is a subset of X^2. X is an *equivalence relation* if it satisfies the following three properties:

(Reflexivity) For all $x \in X$, $(x,x) \in R$.

(Symmetry) For all $x, y \in X$, if $(x,y) \in R$ then $(y,x) \in R$.

(Transitivity) For all $x,y,z \in X$, if $(x,y) \in R$ and $(y,z) \in R$ then $(x,z) \in R$.

(b) One such relation, with the equivalence classes $\{1,2\}$ and $\{3\}$, is

$$R = \{(1,1),(1,2),(2,1),(2,2),(3,3)\}.$$

Question 1(a) is bookwork. Question 1(b) is a case of the expected solution to a coursework question on counting equivalence relations.

Question 2 (a) Use the Euclidean algorithm to compute $\gcd(426,330)$. [6]

(b) Find a solution to the equation

$$426k + 330\ell = \gcd(426,330)$$

where k and ℓ are integers. [8]

Solution (a) Taking remainders, we calculate

$$\begin{aligned} 426 &= 1 \cdot 330 + 96 \\ 330 &= 3 \cdot 96 + 42 \\ 96 &= 2 \cdot 42 + 12 \\ 42 &= 3 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 + 0, \end{aligned}$$

so the greatest common divisor is 6.
(b) Reversing the algorithm,

$$\begin{aligned} 6 &= 42 - 3 \cdot 12 \\ &= 42 - 3(96 - 2 \cdot 42) = -3 \cdot 96 + 7 \cdot 42 \\ &= -3 \cdot 96 + 7(330 - 3 \cdot 96) = 7 \cdot 330 - 24 \cdot 96 \\ &= 7 \cdot 330 - 24(426 - 330) = -24 \cdot 426 + 31 \cdot 330 \end{aligned}$$

and $k = -24$, $\ell = 31$ is a solution.

Both parts of question 2 are standard algorithm-following, with many parallel examples in lecture and coursework.

Question 3 Solve the following system of equations over $\mathbb{Z}_{11}$ for x and y.

$$\begin{aligned} [4]_{11}\, x + [7]_{11}\, y &= [4]_{11} \\ [2]_{11}\, x + [6]_{11}\, y &= [1]_{11}. \end{aligned}$$

Justify your answer. [8]

Solution Here is one of many approaches to solving the system. Solve the second equation for x:

$$\begin{aligned} [2]_{11}\, x &= [1]_{11} - [6]_{11}\, y \\ \implies \qquad x &= [2]_{11}^{-1}\,([1]_{11} - [6]_{11}\, y). \end{aligned}$$

Substitute into the first equation:

$$[4]_{11}\,[2]_{11}^{-1}\,([1]_{11} - [6]_{11}\, y) + [7]_{11}\, y = [3]_{11}.$$

Since $4/2 = 2$ is an integer we may simplify $[4]_{11}\,[2]_{11}^{-1}$ to $[2]_{11}$. Then the above comes out to

$$\begin{aligned} [2]_{11}\,([1]_{11} - [6]_{11}\, y) + [7]_{11}\, y &= [4]_{11} \\ [2]_{11} - [12]_{11}\, y + [7]_{11}\, y &= [4]_{11} \\ -[5]_{11}\, y &= [2]_{11} \\ y &= -[5]_{11}^{-1}[2]_{11} = [6]_{11}^{-1}[2]_{11}. \end{aligned}$$

Recogning that $2 \cdot 6 = 12 \equiv_{11} 1$, this implies $y = [2]_{11}[2]_{11} = [4]_{11}$. Substitute this into the equation for x:

$$x = [2]_{11}^{-1}([1]_{11} - [6]_{11}[4]_{11}) = [2]_{11}^{-1}[-23]_{11} = [2]_{11}^{-1}[10]_{11} = [5]_{11}.$$

As justification we check that these indeed solve the original equations:

$$[4]_{11}[5]_{11} + [7]_{11}[4]_{11} = [48]_{11} = [4]_{11}$$
$$[2]_{11}[5]_{11} + [6]_{11}[4]_{11} = [34]_{11} = [1]_{11}.$$

Question 3 is coursework with different constants.

Question 4 Let f be the following permutation in S_{10}, given in two-line notation.

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

(a) Write f in cycle notation. [3]

(b) Let $g \in S_{10}$ be the element (1)(2 8 6 7)(3 5 4 9)(10), in cycle notation. Determine fg^{-1}, written in cycle notation. [6]

(c) Determine the order of f. [3]

(d) Specify an integer n such that f^n fixes exactly seven elements of the set $\{1,2,\ldots,10\}$. [4]

Solution (a) $f = (1\ 4\ 6)(2\ 7\ 5\ 8\ 10)(3\ 9)$.
(b) $fg^{-1} = (1\ 4\ 8\ 7)(2\ 5\ 9\ 6\ 10)(3)$.
(c) The order of f is the least common multiple of the lengths of its cycles, which is $\mathrm{lcm}(3,5,2) = 30$.
(d) Recall the fact that we used when proving the fact we just used about order: f^n is the product of the n-th power of each of the disjoint cycles in f.

If c is a cycle, then c^n is the identity if n divides the order of c; otherwise, c^n does not fix any of the elements contained in c. So the fixed points of any power of f must be the union of some of its *orbits* (i.e. the elements contained in each of its cycles). Our f has cycles of orders 3, 5, and 2, and the only way to make 7 as the sum of some of these numbers is $7 = 5+2$. So the n we are looking for must be a multiple of 5 and of 2, but not of 3. The simplest solution is $n = 10$; alternatively, any n which is a multiple of 10 but not of 30 would do.

Parts (a)–(c) of question 4 are standard computations. Question 4(d) is unseen.

Question 5 (a) State the definition of the *divisibility relation* $\mid$ on the set of natural numbers. [3]

(b) Prove, using mathematical induction, that

$$12 \mid (7^n - 3^{n+1} + 2)$$

for all natural numbers $n \geq 0$. [9]

Solution (a) If a and b are natural numbers, $a \mid b$ if and only if $b = ca$ for some natural number c.
(b) Let $P(n)$ be the statement $12 \mid (7^n - 3^{n+1} + 2)$. We must prove that $P(0)$ is true and that $P(k)$ implies $P(k+1)$ for $k \geq 0$.

$P(0)$ says
$$12 \mid 7^0 - 3^1 + 2 = 0,$$
which is true.

Suppose that $P(k)$ is true for some k. We would like to prove $P(k+1)$, which says

$$12 \mid 7^{k+1} - 3^{k+2} + 2 = 7(7^k - 3^{k+1} + 2) + 4 \cdot 3^{k+1} - 12. \quad (1)$$

By the inductive hypothesis $P(k)$, 12 divides $7(7^k - 3^{k+1} + 2)$. Because $k \geq 0$, $k+1$ is at least 1 and so $12 = 4 \cdot 3$ divides $4 \cdot 3 \cdot 3^k = 4 \cdot 3^{k+1}$. And of course 12 divides -12. Therefore 12 divides the sum of all three of these terms, which is the right hand side of equation (1). Therefore $P(k+1)$ is true, completing the proof by induction.

Question 5(a) is bookwork. Question 5(b) is unseen though it's an elaboration of similar coursework questions with n appearing only once in the dividend.

Question 6 (a) Let R be a set on which two operations $+$ and $\cdot$ are defined. Define what it means for R to be a *ring*. [4]

(b) Let R be a ring. Prove that, if 0 is the additive identity in R, then $0 \cdot a = 0$ for every element a of R. [4]

(c) Give an example of a ring whose set of elements is finite and in which the commutative law for multiplication does not hold. Justify your answer. [6]

Solution (a) R is a *ring* if the operations satisfy the following laws.
Additive laws:

(Closure) For all $a, b \in R$, we have $a + b \in R$.

(Associativity) For all $a, b, c \in R$, we have $a + (b + c) = (a + b) + c$.

(Identity) There is an element $0 \in R$ with the property that $a + 0 = 0 + a = a$ for all $a \in R$.

(Inverse) For all $a \in R$, there exists an element $b \in R$ such that $a + b = b + a = 0$. We write b as $-a$.

(Commutativity) For all $a, b \in R$, we have $a + b = b + a$.

Multiplicative laws:

(Closure) For all $a, b \in R$, we have $ab \in R$.

(Associativity) For all $a, b, c \in R$, we have $a(bc) = (ab)c$.

Mixed laws:

(Distributivity) For all $a, b, c \in R$, we have $a(b+c) = ab+ac$ and $(b+c)a = ba+ca$.

(b) By the zero law (aka the additive identity law) and distributivity,

$$0a + 0 = 0a = (0+0)a = 0a + 0a.$$

Cancelling $0a$, by adding its additive inverse to both sides and using the additive inverse law, gives

$$0 = -0a + 0a + 0 = -0a + 0a + 0a = 0a.$$

(c) One class of examples of such rings is the ring of matrices of a fixed size at least 2 over $\mathbb{Z}_m$ for $m \geq 2$. One *particular* example is the ring of 2×2 matrices over $\mathbb{Z}_2$.

This ring has finitely many elements because a 2×2 matrix is determined by its four entries, and there are only finitely many choices in $\mathbb{Z}_2$ for each of these entries. (Indeed, it has $2^4 = 16$ elements.)

A counterexample to the commutative law for multiplication is

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

which does not equal

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

(For ease of readability I have written a instead of $[a]_2$ for the matrix entries.)

Questions 6(a,b) are bookwork. Question 6(c) is unseen.

Question 7 (a) Let G be a group. Define what it means to say that a set H is a *subgroup* of G. [3]

(b) Let g and h be elements of a group G. Prove that if $gh = hg$, then $g^{-1}h = hg^{-1}$. [6]

(c) Let G be a group, and h an element of G. Prove that

$$\{g \in G : gh = hg\}$$

is a subgroup of G. [6]

Solution (a) H is a *subgroup* of G if H is a subset of G, and H is a group under the same operation for which G is a group.
(b) Let gh and hg be such elements. Multiply the equation $gh = hg$ by g^{-1} on both sides:

$$hg^{-1} = g^{-1}ghg^{-1} = g^{-1}hgg^{-1} = g^{-1}h,$$

which is what was to be proved.
(c) Let us give this subset the name H. We use the subgroup test: what we must show is that if f and g are elements of H, then so is fg^{-1}. We have

$$\begin{aligned} & fg^{-1}h \\ &= fhg^{-1} && \text{because } g \in H \text{, using part (b)} \\ &= hfg^{-1} && \text{because } f \in H \end{aligned}$$

which proves that $fg^{-1} \in H$, completing the proof.

Question 7(a) is bookwork. I intend that questions 7(b,c) will be coursework.

Question 8 Let the operations of addition and multiplication on the set

$$K = \{at + bu : a, b \in \mathbb{R}\},$$

where t and u are formal symbols, be defined as follows:

$$\begin{aligned} (at + bu) + (ct + du) &= (a + c)t + (b + d)u, \\ (at + bu) \cdot (ct + du) &= (ac + ad + bc - bd)t + (-ac + ad + bc + bd)u. \end{aligned}$$

(a) Compute $(\frac{1}{2}t - \frac{1}{2}u)^2$ and express the result in the form $at + bu$. [3]

(b) Find a multiplicative identity in K, and prove that the multiplication in K satisfies the identity law. [4]

(c) Specify a bijection $f : \mathbb{C} \to K$ such that $f(\alpha + \beta) = f(\alpha) + f(\beta)$ and $f(\alpha\beta) = f(\alpha)f(\beta)$ for all complex numbers α and β. [6]

[Such a bijection is called an *isomorphism* of rings.]

Solution (a) Using the definition of multiplication in K,

$$\begin{aligned} &(\frac{1}{2}t - \frac{1}{2}u)(\frac{1}{2}t - \frac{1}{2}u) = \\ &\quad = (\frac{1}{2}\frac{1}{2} + \frac{1}{2}\frac{-1}{2} + \frac{-1}{2}\frac{1}{2} - \frac{-1}{2}\frac{-1}{2})t + (-\frac{1}{2}\frac{1}{2} + \frac{1}{2}\frac{-1}{2} + \frac{-1}{2}\frac{1}{2} + \frac{-1}{2}\frac{-1}{2})u = \\ &\qquad = -\frac{1}{2}t - \frac{1}{2}u. \end{aligned}$$

(b) If $at+bu$ is a multiplicative identity in K, then $(at+bu)(ct+du) = ct+du$ for all real numbers c and d. Equating coefficients of t and u, this means

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

These equations in $\mathbb{R}$ must be true for any real numbers c and d, so we may equate coefficients of c and d in each equation. This gives

$$\begin{aligned} a+b &= 1 \\ a-b &= 0 \\ -a+b &= 0 \\ a+b &= 1. \end{aligned}$$

This is quickly solved to give $a = b = \frac{1}{2}$. So $\frac{1}{2}t + \frac{1}{2}u$ should be the multiplicative identity. Indeed, it is: for all reals c and d,

$$(\frac{1}{2}t+\frac{1}{2}u)\cdot(ct+du) = (\frac{1}{2}c+\frac{1}{2}d+\frac{1}{2}c-\frac{1}{2}d)t + (-\frac{1}{2}c+\frac{1}{2}d+\frac{1}{2}c+\frac{1}{2}d)u = ct+du$$

and $$(ct+du)\cdot(\frac{1}{2}t+\frac{1}{2}u) = (c\frac{1}{2}+c\frac{1}{2}+d\frac{1}{2}-d\frac{1}{2})t + (-c\frac{1}{2}+c\frac{1}{2}+d\frac{1}{2}+d\frac{1}{2})u = ct+du$$

proving the multiplicative identity law.
(c) We would like $f(1)$ to be $\frac{1}{2}t+\frac{1}{2}u$, the multiplicative identity we found in part (b). The answer we found in part (a) was the negative of the multiplicative identity, so $\frac{1}{2}t-\frac{1}{2}u$ is a good candidate for $f(i)$, being the square root of what should be $f(-1)$. Finally, for addition to be "the same" in K as it is in $\mathbb{C}$, we are led to make the following definition for f:

$$f(a+bi) := a(\frac{1}{2}t+\frac{1}{2}u) + b(\frac{1}{2}t-\frac{1}{2}u) = \frac{a+b}{2}t + \frac{a-b}{2}u.$$

I did not ask for a proof, but here's one. To prove f is injective and surjective reduces to showing that, for all reals c and d,

$$\frac{a+b}{2}t + \frac{a-b}{2}u = ct+du$$

has only one solution. This is true; equating coefficients and solving produces the unique solution $a = c+d$, $b = c-d$.

To prove $f(\alpha+\beta) = f(\alpha)+f(\beta)$, let $\alpha = a+bi$, $\beta = c+di$. Then

$$f(\alpha+\beta) = f(a+c+(b+d)i) = \frac{a+c+b+d}{2}t + \frac{a+c-b-d}{2}u$$

which equals

$$f(\alpha)+f(\beta) = \left(\frac{a+b}{2}t+\frac{a-b}{2}u\right) + \left(\frac{c+d}{2}t+\frac{c-d}{2}u\right) = \frac{a+b+c+d}{2}t + \frac{a-b+c-d}{2}u.$$

Similarly, for multiplication,

$$f(\alpha\beta) = f(ac - bd + (ad + bc)i) = \frac{ac - bd + ad + bc}{2}t + \frac{ac - bd - ad - bc}{2}u$$

equals

$$\begin{aligned}
f(\alpha)f(\beta) &= \left(\frac{a+b}{2}t + \frac{a-b}{2}u\right)\left(\frac{c+d}{2}t + \frac{c-d}{2}u\right) \\
&= \frac{(a+b)(c+d) + (a+b)(c-d) + (a-b)(c+d) - (a-b)(c-d)}{4}t \\
&\quad + \frac{-(a+b)(c+d) + (a+b)(c-d) + (a-b)(c+d) + (a-b)(c-d)}{4}u \\
&= \frac{(1+1+1-1)ac + (1-1+1+1)ad + (1+1-1+1)bc + (1-1-1-1)bd}{4}t \\
&\quad + \frac{(-1+1+1+1)ac + (-1-1+1-1)ad + (-1+1-1-1)bc + (-1-1-1+1)bd}{4}u \\
&= \frac{ac + ad + bc - bd}{2}t + \frac{ac - ad - bc - bd}{2}u.
\end{aligned}$$

All parts of question 8 are unseen, though they have analogues which have been seen, including bookwork and coursework questions about proving field laws in new number systems, and a coursework question about $\{a + bu : a, b \in \mathbb{R}\}, u^2 = 2u + 2$ being isomorphic to $\mathbb{C}$.

End of Paper