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 the definition of a *partition* of a set X. **[3]**

(b) Let $\{A_1, A_2, \dots\}$ be a partition of a set X, and R the relation

$$\{(x,y) \in X^2 : \text{ there exists } j \text{ such that } x \in A_j \text{ and } y \in A_j\}.$$

Prove that R is an equivalence relation. **[6]**

Solution (a) A *partition* of X is a collection $\{A_1, A_2, \dots\}$ of subsets of X having the following properties:

- $A_i \neq \emptyset$ for all i;
- $A_i \cap A_j = \emptyset$ for all $i \neq j$;
- $A_1 \cup A_2 \cup \cdots = X$.

(b) We must prove that this relation is reflexive, symmetric, and transitive.

- x and x lie in the same part of the partition, so R is reflexive.
- If x and y lie in the same part of the partition, then so do y and x; so R is symmetric.
- Suppose that x and y lie in the same part A_i of the partition, and y and z lie in the same part A_j. Then $y \in A_i$ and $y \in A_j$, so $y \in A_i \cap A_j$; so we must have $A_i = A_j$ (since different parts are disjoint). Thus x and z both lie in A_i. So R is transitive.

Thus R is an equivalence relation.
Question 1 is bookwork.

Question 2.

(a) Prove that $[65]_{186}$ has a multiplicative inverse in the ring $\mathbb{Z}_{186}$. **[6]**

(b) Compute this multiplicative inverse. **[8]**

(c) How many of the elements of $\mathbb{Z}_{186}$ have multiplicative inverses? Justify your answer. **[6]**

Solution (a) By a theorem from lectures, $[65]_{186}$ has a multiplicative inverse if and only if $\gcd(65, 186) = 1$. One can prove this by factoring, but since we will need the extended Euclidean algorithm for part (b), we embark on that here. Taking remainders, we calculate

$$\begin{aligned} 186 &= 2 \cdot 65 + 56 \\ 65 &= 1 \cdot 56 + 9 \\ 56 &= 6 \cdot 9 + 2 \\ 9 &= 4 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0, \end{aligned}$$

so the greatest common divisor is 1 and the inverse exists.
(b) Reversing the algorithm,

$$\begin{aligned} 1 &= 9 - 4 \cdot 2 \\ &= 9 - 4(56 - 6 \cdot 9) = -4 \cdot 56 + 25 \cdot 9 \\ &= -4 \cdot 56 + 25(65 - 56) = 25 \cdot 65 - 29 \cdot 56 \\ &= 25 \cdot 65 - 29(186 - 2 \cdot 65) = -29 \cdot 186 + 83 \cdot 65 \end{aligned}$$

and $[65]_{186}^{-1} = [83]_{186}$.
(c) This number is Euler's totient function evaluated at $186 = 2 \cdot 3 \cdot 31$, namely $\phi(186) = (2-1)(3-1)(31-1) = 60$.
Question 2 is a standard computation, exampled in coursework and in lectures with different constants.

Question 3. Let f be the permutation $(1\ 10\ 3\ 9\ 7\ 4)(2)(5\ 11\ 8)(6)$ in S_{11}, which is written in cycle notation.

(a) Write f in two-line notation. **[3]**

(b) Let g be the element

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 2 & 8 & 5 & 1 & 6 & 4 & 11 & 9 & 7 & 10 & 3 \end{pmatrix}$$

of S_{11}, written in two-line notation. Determine $(gf)^{-1}$, and write your answer in cycle notation. **[6]**

(c) Write down an element of S_{11} of order 21. **[4]**

Solution (a)

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 10 & 2 & 9 & 1 & 11 & 6 & 4 & 5 & 7 & 3 & 8 \end{pmatrix}$$

(b) We first compute gf. The result can be written down directly in cycle notation: to produce the cycle containing 1 we write down $1, gf(1), gf(gf(1))$, etcetera, until we recover 1 again; then we repeat this process for each element not yet encountered. This yields $gf = (1\ 10\ 5\ 3\ 7)(2\ 8\ 6\ 4)(9\ 11)$. The inverse is computed by reversing all cycles, so $(gf)^{-1} = (1\ 7\ 3\ 5\ 10)(2\ 4\ 6\ 8)(9\ 11)$.
(c) The order of an element is the lcm of the lengths of its cycles. Since $21 = 7 \cdot 3$, an element that will suffice is $(1\ 2\ 3\ 4\ 5\ 6\ 7)(8\ 9\ 10)(11)$.
Parts (a,b) of Question 3 are standard computations. Part (c) is unseen, though computing the order of a permutation is equally standard.

Question 4.

(a) State the definition of the complex number $\mathrm{e}^{\mathrm{i}\theta}$, where θ is a real number. **[2]**

(b) Prove that $\mathrm{e}^{\mathrm{i}\theta} \cdot \mathrm{e}^{\mathrm{i}\phi} = \mathrm{e}^{\mathrm{i}(\theta+\phi)}$ for all real numbers θ and ϕ. **[4]**

(c) Prove by mathematical induction, or otherwise, that for all integers $n \geqslant 1$,

$$\cos(1) + \cos(2) + \cdots + \cos(n-1) = \frac{\cos(n) - \cos(n-1)}{2\cos(1) - 2} - \frac{1}{2}.$$ **[9]**

Solution (a) $e^{i\theta} = \cos\theta + i\sin\theta$.
(b) The left hand side is

$$(\cos\theta + i\sin\theta)(\cos\phi + i\sin\phi) = \cos\theta\cos\phi - \sin\theta\sin\phi + i(\cos\theta\sin\phi + \sin\theta\cos\phi).$$

Using trigonometric sum formulae, this is

$$\cos(\theta+\phi) + i\sin(\theta+\phi)$$

which is the right hand side.
(c) We give the proof by induction. Recognition as the real part of a geometric series is also possible.
The base case is $n = 1$, at which the left hand side is an empty sum, evaluating to 0, which is also the evaluation $\frac{1}{2} - \frac{1}{2}$ of the right hand side.
For the inductive hypothesis, let $P(n)$ be the identity to be proved for all n. Assume $P(k)$ is true; we wish to show $P(k+1)$. It is enough to prove the equation resulting from subtracting $P(k)$ from $P(k+1)$, which is

$$\cos(k) = \frac{\cos(k+1) - \cos(k) - (\cos(k) - \cos(k-1))}{2\cos(1) - 2}.$$

It is equivalent to show that

$$2\cos(k)\cos(1) = \cos(k+1) + \cos(k-1),$$

as this implies the equation above upon subtracting $2\cos(k)$ from each side and then dividing both sides by the real number $2\cos(1)-2$, which is nonzero. This last equation is seen to be true on expanding the right hand side using angle sum formulae:

$$\begin{aligned}\cos(k+1)+\cos(k-1) &= \cos(k)\cos(1)-\sin(k)\sin(1)+\cos(k)\cos(-1)-\sin(k)\sin(-1)\\ &= 2\cos(k)\cos(1)\end{aligned}$$

because cos is an even function and sin an odd one. This completes the inductive step and thus the proof.
Parts (a,b) of Question 4 are bookwork. Part (c) is unseen.

Question 5.

(a) Let R be a ring. Prove that $-(ab) = (-a)\cdot b$ for any elements $a, b \in R$. **[6]**

(b) Let R be a ring, and define the relation $\mid$ on R so that, if a and b are elements of R, then $a \mid b$ if and only if $b = ra$ for some $r \in R$. Must the relation $\mid$ be reflexive? symmetric? transitive? Prove your assertions. **[6]**

Solution (a) We know by a lemma proved in lectures that $0b = 0$ for any $b \in R$. I will make use of this here.
The defining property of the element $-a$, given by the additive inverse law, is

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

Multiplying by b yields

$$0 = 0b = (a+(-a))b = ab + (-a)b$$

using distributivity and our lemma about multiplication by 0. The result now follows by adding the additive inverse of ab to both sides:

$$-(ab) = -(ab) + 0 = -(ab) + ab + (-a)b = (-a)b.$$

(b) The relation $\mid$ need not be reflexive, notionally because rings without identity exist. For instance, $2 \nmid 2$ in the ring $2\mathbb{Z}$.
The relation $\mid$ is scarcely ever symmetric. For instance, in any ring with identity, $1 \mid 0$ but $0 \nmid 1$.
The relation $\mid$ must be transitive. Suppose $a \mid b$ and $b \mid c$, that is, $b = ra$ and $c = sb$ for some $r, s \in R$. Then $c = s(ra) = (sr)a$ by associativity, implying $a \mid c$.
Question 5(a) is coursework. Question 5(b) is unseen, though the same question over the ring $\mathbb{Z}$ is bookwork.

Question 6. Let S be the subset of $\mathrm{M}_2(\mathbb{C})$ consisting of matrices of the form

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}.$$

(a) Prove that S is closed under addition and multiplication. **[4]**

(b) Prove that S satisfies the multiplicative inverse law. You may assume that $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the multiplicative identity in S. **[6]**

(c) Prove that S is not a field. **[6]**

Solution (a) The sum of two arbitrary elements $\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}$ and $\begin{pmatrix} \gamma & \delta \\ -\bar{\delta} & \bar{\gamma} \end{pmatrix}$ of S is

$$\begin{pmatrix} \alpha+\gamma & \beta+\delta \\ -\overline{\beta+\delta} & \overline{\alpha+\gamma} \end{pmatrix}$$

which is visibly in S. Their product is

$$\begin{pmatrix} \alpha\gamma-\beta\bar{\delta} & \alpha\delta+\beta\bar{\gamma} \\ -\bar{\beta}\gamma-\bar{\alpha}\bar{\delta} & -\bar{\beta}\delta+\bar{\alpha}\bar{\gamma} \end{pmatrix} = \begin{pmatrix} \alpha\gamma-\beta\bar{\delta} & \alpha\delta+\beta\bar{\gamma} \\ -\overline{\alpha\delta+\beta\bar{\gamma}} & \overline{\alpha\gamma-\beta\bar{\delta}} \end{pmatrix}$$

which is also in S.

(b) Suppose α and β are not both 0, and write $q = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}$. Then

$$r := \frac{1}{|\alpha|^2+|\beta|^2}\begin{pmatrix} \bar{\alpha} & -\beta \\ \bar{\beta} & \alpha \end{pmatrix}$$

is in S, and one computes

$$qr = rq = \frac{1}{|\alpha|^2+|\beta|^2}\begin{pmatrix} \alpha\bar{\alpha}+\beta\bar{\beta} & 0 \\ 0 & \alpha\bar{\alpha}+\beta\bar{\beta} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

(Of course, r is also the inverse of q within $M_2(\mathbb{C})$.)

(c) S is not a field because its multiplication is not commutative. For instance, the matrices $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ both lie in S and fail to commute:

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

which is unequal to

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

Question 6 is unseen in this form, though there is a coursework question etablishing that S is isomorphic as a ring to the quaternions.

Question 7.

(a) Define what it means for a set G with an operation $\circ$ to be a *group*. **[3]**

(b) Give an example of two finite groups which have the same order but are not isomorphic. **[6]**

(c) Let R be a ring with identity. Prove that the set $R^\times$ of units of R, with the operation of multiplication, is a group. **[6]**

Solution (a) G is a group under $\circ$ iff it satisfies the following axioms:

(G0) Closure law: for all $a,b \in G$, we have $a \circ b \in G$.

(G1) Associative law: for all $a,b,c \in G$, we have $a \circ (b \circ c) = (a \circ b) \circ c$.

(G2) Identity law: there is an element $e \in G$ (called the *identity*) such that $a \circ e = e \circ a = a$ for any $a \in G$.

(G3) Inverse law: for all $a \in G$, there exists $b \in G$ such that $a \circ b = b \circ a = e$, where e is the identity. The element b is called the *inverse* of a, written a'.

(b) S_3 has order $3! = 6$, as does the additive group $\mathbb{Z}_6$, but the latter is abelian and the former is not, so they cannot be isomorphic.
(c)We must prove the laws from part (a).
Suppose that u^{-1} and v^{-1} are the inverses of u and v. Then

$$\begin{aligned}(uv)(v^{-1}u^{-1}) &= u(vv^{-1})u^{-1} = u1u^{-1} = uu^{-1} = 1,\\ (v^{-1}u^{-1})(uv) &= v^{-1}(u^{-1}u)v = v^{-1}1v = v^{-1}v = 1,\end{aligned}$$

so $v^{-1}u^{-1}$ is the inverse of uv. Thus the closure law holds for $R^\times$.
The associative law for $R^\times$ is inherited from R, of which it is a subset.
The equation $1 \cdot 1 = 1$ shows that 1 is the inverse of 1, so that $1 \in R^\times$. This element 1 is still an identity in $R^\times \subseteq R$, so $R^\times$ satisfies the identity law.
If $u \in R^\times$, the equation $u^{-1}u = uu^{-1} = 1$, which holds because u^{-1} is the inverse of u, also shows that u is the inverse of u^{-1}. Thus $u^{-1} \in R^\times$, inside which it is still the inverse of u, showing that $R^\times$ satisfies the inverse law.
Question 7 is bookwork.

End of Paper.