Queen Mary
University of London

MTH4104: Introduction to Algebra

Duration: 2 hours

Date and time: TBD

Model solutions

Question 1.

(a) Let g be the element

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

of S_{10}, written in two-line notation. Write g in cycle notation. **[3]**

(b) What are the fixed points of g? **[2]**

(c) Find an element h of S_{10} such that

$$h \circ g = (1\ \ 8\ \ 10\ \ 2\ \ 7\ \ 3\ \ 6\ \ 4),$$

and write it in two-line notation. **[6]**

(d) Does S_{10} contain an element of order 30? If so, specify one. If not, explain why. **[4]**

Solution (a) $g = (1\ \ 6\ \ 9\ \ 3\ \ 10\ \ 8\ \ 7)(4\ \ 5)$.
(b) 2 is the only fixed point of g.
(c) If we name the displayed eight-cycle k, then the element we seek is $h = kg^{-1}$. We invert g by turning its cycles backwards, giving $g^{-1} = (1\ \ 7\ \ 8\ \ 10\ \ 3\ \ 9\ \ 6)(4\ \ 5)$. We can compute kg^{-1} and write the result in cycle notation directly: to produce the cycle containing 1 we write down 1, $kg^{-1}(1)$, $kg^{-1}(kg^{-1}(1))$, etcetera, until we recover 1 again; then we repeat this process for each element not yet encountered. This yields $kg^{-1} = (1\ \ 3\ \ 9\ \ 4\ \ 5)(2\ \ 7\ \ 10\ \ 6\ \ 8)$. In two-line notation that is

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

(d) The order of an element is the lcm of the lengths of its cycles. Since $30 = 5 \cdot 3 \cdot 2$, an element that will suffice is $(1\ \ 2\ \ 3\ \ 4\ \ 5)(6\ \ 7\ \ 8)(9\ \ 10)$.
Parts (a,b,c) of Question 1 are standard computations. Part (d) is unseen, though computing the order of a permutation is equally standard.

Question 2.

(a) State the **Fundamental Theorem of Algebra**. **[3]**

(b) Find all solutions to the complex polynomial equation

$$z^4 + 8 - 8\sqrt{3}\mathrm{i} = 0,$$

and write them in standard form $a + b\mathrm{i}$. **[9]**

Solution (a) Here is how it's phrased in the notes:

Let $a_0, a_1, \cdots, a_{n-1}$ be complex numbers. The polynomial equation

$$z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 = 0$$

has at least **one** solution inside $\mathbb{C}$.

Also acceptable are more allegro phrasings, like "Every non-constant complex polynomial has a zero" (but *non-constant* is essential), and assertions that there are n roots counted with multiplicity (but mention of the multiplicity is essential).
(b) We know a method for taking roots of complex numbers, so we convert the equation to that form

$$z^4 = -8 + 8\sqrt{3}\mathrm{i}$$

We will use the modulus-argument form $z = re^{i\theta}$ for z, so the first task is to put $-8 + 8\sqrt{3}\mathrm{i}$ in this form. If $-8 + 8\sqrt{3}\mathrm{i} = se^{\mathrm{i}\phi}$, then s is the modulus,

$$s = |-8 + 8\sqrt{3}\mathrm{i}| = \sqrt{(-8)^2 + (8\sqrt{3})^2} = 16,$$

implying $e^{i\phi} = (-8 + 8\sqrt{3}\mathrm{i})/16 = -1/2 + 3\sqrt{2}\mathrm{i}$. Using the Argand diagram, or equating coefficients in the equation $\cos\phi + i\sin\phi = -1/2 + 3\sqrt{2}\mathrm{i}$, we see that we may take $\phi = 2\pi/3$. (Or $\phi = -4\pi/3$, vel sim.)
Therefore the equation to be solved is

$$(re^{\mathrm{i}\theta})^4 = 16e^{\mathrm{i}\cdot 2\pi/3},$$

i.e.

$$r^4 e^{\mathrm{i}\cdot 4\theta} = 16e^{\mathrm{i}\cdot 2\pi/3},,$$

These two quantities are equal when $r^4 = 16$ and $4\theta = 2\pi/3 + 2\pi k$ for some integer k. The first equation implies $r = \sqrt[4]{16} = 2$. The second implies that

$\theta = \pi/6 + \pi k/2$, and since $e^{i\theta}$ has period 2π we only need to take four values of θ, namely

$$\theta = \frac{\pi}{6}, \quad \theta = \frac{2\pi}{3}, \quad \theta = \frac{7\pi}{6}, \quad \theta = \frac{5\pi}{3},$$

corresponding to $k = 0$, 1, 2, and 3 respectively. (If you prefer to take θ in the range $(-\pi, \pi]$ that's okay too; you would use $k = -2, -1, 0, 1$.) So the four solutions are

$$z = 2e^{\mathrm{i}\cdot\pi/6} = 2(\cos\frac{\pi}{6} + \mathrm{i}\sin\frac{\pi}{6}) = 2(\frac{\sqrt{3}}{2} + \frac{1}{2}\mathrm{i}) = \sqrt{3} + \mathrm{i}$$

and

$$z = 2e^{\mathrm{i}\cdot 2\pi/3} = 2(\cos\frac{2\pi}{3} + \mathrm{i}\sin\frac{2\pi}{3}) = (-\frac{1}{2} + \frac{\sqrt{3}}{2}\mathrm{i}) = -1 + \sqrt{3}\mathrm{i}$$

and

$$z = 2e^{\mathrm{i}\cdot 7\pi/6} = 2(\cos\frac{7\pi}{6} + \mathrm{i}\sin\frac{7\pi}{6}) = 2(-\frac{\sqrt{3}}{2} - \frac{1}{2}\mathrm{i}) = -\sqrt{3} - \mathrm{i}$$

and

$$z = 2e^{\mathrm{i}\cdot 5\pi/3} = 2(\cos\frac{5\pi}{3} + \mathrm{i}\sin\frac{5\pi}{3}) = 2(\frac{1}{2} - \frac{\sqrt{3}}{2}\mathrm{i}) = 1 - \sqrt{3}\mathrm{i}.$$

Part (a) of Question 2 is bookwork, and part (b) is a standard algorithm.

Question 3.

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

(b) Write out the Cayley table for the multiplicative group $\mathbb{Z}_8^\times$. **[3]**

(c) Does the additive group $\mathbb{Z}_{30}$ have a subgroup of order 4? Specify one if so, or explain why if not. **[4]**

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'.

Omitting the closure law is fine too.
(b)

	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$[1]_8$	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$[3]_8$	$[3]_8$	$[1]_8$	$[7]_8$	$[5]_8$
$[5]_8$	$[5]_8$	$[7]_8$	$[1]_8$	$[3]_8$
$[7]_8$	$[7]_8$	$[5]_8$	$[3]_8$	$[1]_8$

(c) There is no such subgroup, by Lagrange's theorem: if G is such a subgroup of $\mathbb{Z}_{30}$, then $4 = |G| \mid |\mathbb{Z}_{30}| = 30$, which is false.
Part (a) is bookwork. Parts (b,c) are familiar types of exercise.

Question 4.

(a) State the names of the axioms that must hold of a set R with operations $+$ and $\cdot$ in order for R to be a **ring**. **[3]**

(b) Define what it means for an element of a ring with identity to be a **unit**. **[2]**

(c) Is $2 - 2t$ a unit in the ring $\mathbb{D}$ of pseudocomplex numbers? Justify your answer. **[4]**

(d) Let a be an element of a ring R with identity such that $a^n = 0$ for some natural number n. Prove that $1 - a$ is a unit in R. **[5]**

Solution (a) A ring must satisfy the associative, identity, inverse and commutative laws for addition, the associative law for multiplication, and the distributive law. (Mentioning the closure laws too is acceptable, although they are implicit in the definition of the operations.)
(b) An element x of R is a unit if it has a multiplicative inverse.
(c) $2 - 2t$ is not a unit. Suppose it had a multiplicative inverse $a + bt$ where $a, b \in \mathbb{R}$. Expanding

$$(2 - 2t)(a + bt) = 1 + 0t$$

gives

$$2a - 2b + (-2a + 2b)t = 1 + 0t$$

which, by extracting coefficients, yields the system

$$\begin{aligned} 2a - 2b &= 1 \\ -2a + 2b &= 0. \end{aligned}$$

This is an inconsistent system, as adding the two equations yields $0 = 1$. So the inverse cannot exist.
(d) An inverse of $1 - a$ is $1 + a + \cdots + a^{n-1}$, since

$$(1-a)(1+a+\cdots+a^{n-1}) = 1+a+\cdots+a^{n-1}-a-a^2-\cdots-a^n = 1-a^n = 1$$

and similarly

$$(1 + a + \cdots + a^{n-1})(1 - a) = 1 - a + a - a^2 + \cdots + a^{n-1} - a^n = 1 - a^n = 1.$$

Parts (a,b) of question 4 are bookwork. Part (c) is an exercise with parallels in lecture. Part (d) is unseen.

Question 5.

(a) Give complete definitions of the terms

(i) **Cartesian product** of two sets; **[2]**

(ii) **relation** on a set; **[2]**

(iii) **equivalence relation** on a set. **[3]**

(b) Write down examples of:

(i) a relation which is transitive but not reflexive; **[2]**

(ii) an equivalence relation on $\{1, 2, 3, 4\}$ with exactly three equivalence classes. **[2]**

(c) Let X and Z be any two sets, and $f : X \to Z$ any function. Prove that

$$\{(x, y) \in X^2 : f(x) = f(y)\}$$

is an equivalence relation on X. **[6]**

Solution (a) The Cartesian product of two sets X and Y is the set

$$X \times Y = \{(x, y) : x \in X, y \in Y\}.$$

A relation on a set X is a subset of $X \times X$. A relation R on X is an equivalence relation if it satisfies the following three properties:

reflexivity: $(x, x) \in R$ for all $x \in X$;

symmetry: $(x, y) \in R$ implies that $(y, x) \in R$;

transitivity: $(x, y) \in R$ and $(y, z) \in R$ together imply that $(x, z) \in R$.

(b) The relation $>$ on the integers is transitive but not reflexive. One equivalence relation on $\{1, 2, 3, 4\}$ with three equivalence classes is

$$\{(1, 1), (1, 4), (2, 2), (3, 3), (4, 1), (4, 4)\},$$

the restriction of $\equiv_3$ to that set. (There are of course other possibilities in each case.)
(c) *Reflexivity*. For any $x \in X$, $f(x) = f(x)$ is true, so xRx.
Symmetry. Let $x, y \in X$ satisfy xRy, so $f(x) = f(y)$. Equality is symmetric so this implies $f(y) = f(x)$, which is yRx.
Transitivity. Let $x, y, z \in X$ satisfy xRy and yRz, so $f(x) = f(y)$ and $f(y) = f(z)$. Then

$$f(x) = f(y) = f(z)$$

so xRz.
Part (a) of Question 5 is bookwork. Part (b) is not seen as such, but the examples are intended to be familiar ones. Part (c) is unseen but a proof which runs along very standard lines; it would be a very easy exemplar of the class if not for the greater generality.

Question 6.

(a) Using the Euclidean algorithm, show that $\gcd(68, 183) = 1$. **[6]**

(b) Does $[68]_{183}$ have a multiplicative inverse in the ring $\mathbb{Z}_{183}$? Find it if so, or explain why if not. **[8]**

(c) Prove that $\mathbb{Z}_m$ is not a field if m is a composite number. (You may assume that $\mathbb{Z}_m$ is a ring, and that its operations are well-defined, but do not use other facts about $\mathbb{Z}_m$ without proof.) **[6]**

Solution (a) We carry out the algorithm, dividing and extracting remainders until we see a remainder of zero:

$$\begin{aligned} 183 &= 2 \cdot 68 + 47 \\ 68 &= 1 \cdot 47 + 21 \\ 47 &= 2 \cdot 21 + 5 \\ 21 &= 4 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 + 0. \end{aligned}$$

The last non-zero remainder, here 1, is the gcd yielded by the algorithm.
(b) If b is an integer such that $68b + 183k = 1$ for some integer k, then $[b]_{183}$ will be the inverse sought. The extended Euclidean algorithm guarantees that b exists, and indeed produces it. We run the algorithm by solving for 1 in terms of 68 and 183 with iterated substitution of the equations from part (a):

$$\begin{aligned} 1 &= 21 - 4 \cdot 5 \\ &= 21 - 4 \cdot (47 - 2 \cdot 21) = -4 \cdot 47 + (1 + 2 \cdot 4) \cdot 21 = -4 \cdot 47 + 9 \cdot 21 \\ &= -4 \cdot 47 + 9 \cdot (68 - 1 \cdot 47) = 9 \cdot 68 - (4 + 9 \cdot 1) \cdot 47 = 9 \cdot 68 - 13 \cdot 47 \\ &= 9 \cdot 68 - 13(183 - 2 \cdot 68) = -13 \cdot 183 + (9 + 13 \cdot 2) \cdot 68 = -13 \cdot 183 + 35 \cdot 68. \end{aligned}$$

So our inverse is $[b]_{183} = [35]_{183}$.
(c) Let $m = ab$ where $a, b > 1$ are integers. If $[a]_m$ is to have an inverse $[c]_m$, this implies that $[a]_m[c]_m = [ac]_m$ is the same congruence class as $[1]_m$, i.e. that $ac \equiv_m 1$, i.e. that $ac - km = 1$ for some k. But a divides the left side of this equality and not the right, which is a contradiction.
Parts (a,b) of Question 6 are standard algorithms. Part (c) is bookwork.

Question 7. Let T be the set of real numbers. Consider T as an algebraic structure with addition operation $\oplus$ and multiplication operation $\odot$ given by

$$\begin{aligned} x \oplus y &= \min\{x, y\}, \\ x \odot y &= x + y - 2. \end{aligned}$$

(a) Name the identity element in T for the operation $\odot$, and prove the inverse law for $\odot$. **[4]**

(b) Prove the distributive law in T. [Hint: consider two cases $x \leq y$, $x > y$.] **[3]**

(c) Prove that the set T with addition $\oplus$ and multiplication $\odot$ is not a ring. **[5]**

Solution (a) The identity element for $\odot$ is 2, because

$$x \odot 2 = x + 2 - 2 = x$$

for all real x (and similarly for $2 \odot x$). The inverse of any real number x under $\odot$ is $4 - x$, because

$$x \cdot (4 - x) = x + 4 - x - 2 = 2$$

(and similarly for $(4 - x) \odot x$). This proves the inverse law for $\odot$.
(b) Since $\odot$ is commutative (by inspection), it is sufficient for us to check one of the two distributive laws. So let $x, y, z \in T$. We must prove the equality of

$$(x \oplus y) \odot z = \min\{x, y\} + z - 2$$

and

$$(x \odot z) \oplus (y \odot z) = \min\{x + z - 2, y + z - 2\}.$$

We take two cases according to whether $x \leq y$ or $x > y$. In the first case, adding $z + 2$ to both sides of the inequality gives $x + z - 2 \leq y + z - 2$, so the two displayed quantities both come out to $x + z - 2$. By similar reasoning, in the second case both displayed quantities are $y + z - 2$. In either event, they are equal.
(c) T is not a ring because it fails to satisfy the additive identity law. Indeed, there can be no additive identity element e, because

$$e \oplus (e + 1) = \min\{e, e + 1\} = e$$

is not equal to $e + 1$.
Question 7 is wholly unseen. Various examples of proving and disproving laws in number systems have been seen, but none have had quite this flavour.

End of Paper.