Manchester Metropolitan University

Mock Examination
Faculty Of Science & Engineering
Department Of Computing And Mathematics
MATHEMATICS UNDERGRADUATE NETWORK
Level 5

Mock examination with solutions for

6G5Z0048 Number Theory and Abstract Algebra

Duration : 3 hours

Instructions to students

- You need to answer **FIVE** questions. This must include **TWO** questions from Section A and **TWO** questions from Section B. Your fifth question can then come from any of the remaining questions.
- If you answer more than five questions then you will get the marks from your best five questions, subject to the sectioning requirements above.
- You must show all of your working and explain your reasoning carefully to gain full marks.
- Marks awarded for each question part are shown in square brackets aligned to the right-hand margin.

Permitted materials

- Students are permitted to use their own calculators without mobile communication facilities.

SECTION A – Number Theory questions

1. (a) State precisely the definition of the divisibility relation $a\,|b$ on the integers and use it to prove that for all $a, b, c \in \mathbb{Z}$, if $a\,|b$ and $a\,|c$ then for all $m, n \in \mathbb{Z}$, [6]

$$a\,|(mb + nc).$$

Solution: We say a divides b, and write $a|b$, if and only if there exists an integer c such that $b = ac$.

3 for the def. of divisibility

Let us assume that $a|b$ and $a|c$, i.e. there exist integers $beta, \gamma$ such that $b = a\beta$ and $c = a\gamma$. Then we can say

$$\begin{aligned} mb + nc &= ma\beta + na\gamma \\ &= a(m\beta + n\gamma). \end{aligned}$$

$m\beta + n\gamma$ is clearly an integer, so by definition, we have $a|(mb + nc)$.

3 for this proof

(b) Use the principle of mathematical induction to prove that [5]

$$\forall n \geq 1 \quad 7\,|\left(2^{3n} - 1\right).$$

You should point out in your argument where you make use of the linear combinations result from part (a) above.

Solution: When $n = 1$, $2^{3n} - 1 = 7$, and clearly $7|7$. So the base case is true. Let us assume that $7|2^{3k} - 1$, for some $k \geq 1$, and then note that

$$\begin{aligned} 2^{3(k+1)} - 1 &= 8 \cdot 2^{3k} - 1 \\ &= 8 \cdot (2^{3k} - 1) + 7. \end{aligned}$$

Note that this last expression is a linear combination of integers divisible by 7, so by part (a) we have $7|(2^{3(k+1)} - 1)$. Hence, by induction, $7\,|\left(2^{3n} - 1\right)$ for all $n \geq 1$.

1 for base case
2 for assumption step
2 for completion

(c) Write down the definition of $\gcd(a, b)$. What relation does it have to the set of linear combinations of a and b with integer coefficients? [5]

Solution: The greatest common divisor, $\gcd(a, b)$, of a and b, is the largest integer d, such that $d|a$ and $d|b$.

3 for the definition

It is also the smallest positive integer that is a linear combination of a and b with integer coefficients, i.e.

$$\gcd(a, b) = \min_{\alpha,\beta\in\mathbb{Z}} \{\alpha a + \beta b \,|\, \alpha a + \beta b > 0\}.$$

2 for this connection

(d) Prove that for all $a, b, c \in \mathbb{Z}$, if $\gcd(a, b) = 1$ and $a|c$ and $b|c$, then $ab|c$. [4]

Solution: By part (c), since $\gcd(a,b)=1$ there exist $\alpha,\beta\in\mathbb{Z}$ such that $\alpha a+\beta b=1$. This implies that $c=\alpha ac+\beta bc$. Now since $a|c$ and $b|c$ we can say that $ab|bc$ and $ab|ac$ and so $ab|c$, as required.

4 for this proof

2. (a) Prove that there are infinitely many prime numbers. State clearly any results about divisibility that you rely on. [10]

Solution: We present Euclid's proof by contradiction. Assume, on the contrary, that there are only a finite number of primes, and that they can be listed as $p_1, p_2, \ldots, p_n$.

2 for beginning proof by contradiction

Then consider the integer N defined by

$$N=\left(\prod_{i=1}^{n} p_i\right)+1.$$

2 for correct large integer

By the Fundamental theorem of arithmetic N factorizes uniquely into primes, so we can say that there is some j, with $1\leq j\leq n$ and $p_j|N$.

2 for obtaining divisibility by a prime

Rewriting the above equation as

$$1=N-\left(\prod_{i=1}^{n} p_i\right),$$

we see that $p_j|1$ as 1 is a linear combination of integers, both divisible by p_j.

2 for obtaining divisibility of 1

But $p_j|1$ contradicts the fact that $p_j>1$ as p_j is prime.

So we conclude that there are infinitely many primes.

2 for obtaining contradiction and completion

(b) Euclid's lemma states that for all primes p and for all $a,b\in\mathbb{Z}$, if $p|ab$ then $p|a$ or $p|b$. Prove this lemma. State any results about divisibility or greatest common divisors that you rely on. [6]

Solution: Let p be a prime and assume that $p|ab$. If $p|a$ we are done.

2 for initiating proof with good structure.

Otherwise, we can assume that $p\not| a$ which means $gcd(a,p)=1$, since p is prime. Then there exist $\alpha,\pi\in\mathbb{Z}$ such that $\alpha a+\pi p=1$. This implies that $\alpha ab+\pi pb=b$ and hence $p|b$ since b is written as a linear combination of integers divisible by p, namely ab and p.

4 for completion.

So Euclid's lemma is proved, either $p|a$ or $p|b$.

(c) Prove that if an integer of the form $2^m + 1$ is prime then it must be the case that $n = 2^m$ for some positive integer m. [4]

Solution: We prove the contrapositive.

1 for setting this out

Assume that m is not a power of 2, i.e. that $m = 2^r s$ for integers $r > 0$ and an odd $s > 1$.

1 for clear beginning

Then we can factorize $2^m + 1$ as

$$\begin{aligned} 2^m + 1 &= 2^{2^r s} + 1 \\ &= \left(2^{2^r}\right)^s - (-1)^s \\ &= \left(2^{2^r} + 1\right) \sum_{j=0}^{s-1} \left(2^{rj}(-1)^j\right) \end{aligned}$$

The conditions on r, s imply that this is a genuine factorization, i.e. $1 < 2^{2^r} + 1 < 2^m + 1$, and hence $2^m + 1$ is not prime.

2 for completion

SECTION A – Number Theory questions

3. (a) Carefully state the definition of the congruence relation $a \equiv b \pmod{n}$. How does it relate to the smallest positive remainders left by a and b upon division by n? [3]

> **Solution:** The definition of $a \equiv b \pmod{n}$ is that $n|(a-b)$.
>
> *2*
>
> And $a \equiv b \pmod{n}$ is equivalent to a and b leaving the same remainder upon division by n.
>
> *1*

(b) Suppose that $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$. Prove that [10]

$$a + b \equiv a' + b' \pmod{n} \text{ and } ab \equiv a'b' \pmod{n}.$$

> **Solution:** We assume that $a \equiv a'$ and $b \equiv b' \pmod{n}$ and so this means that $n|(a-a')$ and $n|(b-b')$. The required results follow from the expressions
>
> $$a + b - (a' + b') = (a - a') - (b - b'),$$
>
> and
>
> $$ab - a'b' = (a - a')(b - b') + a'(b - b') + b'(a - a'),$$
>
> since both the right hand sides are expressed as linear combinations, with integer coefficients, of integers divisible by n, so therefore both $ab - a'b'$ and $a + b - (a' + b')$ are divisible by n, and hence the desired congruences follow.
>
> *5 marks for each result*

(c) Carefully state the definition of the Euler totient function ϕ and prove that for any prime p and positive integer n, that ϕ satisfies [7]

$$\phi(p^n) = p^{n-1}(p-1).$$

> **Solution:** The definition of $\phi(m)$ is the number of integers j such that $1 \leq j \leq m$ and $\gcd(j, m) = 1$.
>
> *2 for definition*
>
> Of the integers j integers j in the range $1 \leq j \leq p^n$, the ones that are not coprime to p^n are those integers j such that $p|j$. This is because p is a prime so the only divisors of p^n are other powers of p.
>
> *2 for hitting this **divisibility by p point***
>
> Within the sequence $1, 2, 3 \ldots, p^n$ the multiples of p are $p, 2p, 3p, \ldots, p^{n-1}p$, so there are p^{n-1} of these, and so the number of j that **are** coprime to p^n is
>
> $$\begin{aligned}\phi(p^n) &= p^n - p^{n-1}\\ &= p^{n-1}(p-1),\end{aligned}$$
>
> as required.
>
> *3 for completion*

4. (a) Consider the congruence [7]

$$45x \equiv 15 \pmod{125}.$$

User relevant result(s) from the theory of congruences to find all the solutions.

Solution: Firstly, $\gcd(45, 125) = 5$ and $5|15$ so by the theorem on linear congruences there do exist solutions and there are five solutions modulo 125.

2 for applying this result

The solutions will be given by

$$t + 25i \pmod{125}, \quad i = 0, 1, 2, 3, 4,$$

where t is the unique solution modulo $125/5 = 25$ to the reduced congruence

$$9x \equiv 3 \pmod{25}.$$

So $t \equiv 9^{-1} \cdot 3 \pmod{25}$.

3 or these applications

The inverse for 9 can be obtained from the extended Euclidean algorithm for $\gcd(9, 25) = 1$,

$$\begin{aligned} 25 &= 2 \cdot 9 + 7 \\ 9 &= 1 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1. \end{aligned}$$

And from these we get the Bezout's identity

$$(-11) \cdot 9 + 4 \cdot 25 = 1,$$

and so $9^{-1} \equiv -11 \equiv 14 \pmod{25}$ and $t \equiv 14 \cdot 3 \equiv 42 \equiv 17 \pmod{25}$. So the solutions are

$$\begin{aligned} x &\equiv 17 + 25i, \quad i = 0, 1, 2, 3, 4, \\ &\equiv 17, 42, 67, 92, 117 \pmod{125} \end{aligned}$$

2 for completion and correctness

(b) Discuss the role played by the Chinese Remainder Theorem in the solution of a general polynomial congruence of the form [5]

$$f(x) \equiv 0 \pmod{n}.$$

You do not need to prove the theorem. Give a general outline of how the theorem is used in combination with other results to solve such a congruence.

Solution: If f is a polynomial with integer coefficients then an integer x is a solution to

$$f(x) \equiv 0 \pmod{n}, \tag{1}$$

if and only if x is a simultaneous solution to

$$f(x) \equiv 0 \pmod{p_i^{a_i}}, \quad i = 1, \ldots r, \tag{2}$$

where the prime factorisation of n is

$$n = \prod_{i=1}^{r} p_i^{a_i}.$$

For each i, the congruence in equation (2) can be solved using the solution lifting technique.

2 for these points

Then solutions to the congruence in (1) are obtianed as follows. Let α_i be a solution to the congruence in (2) for each $i = 1, \ldots, r$. Then we can use the Chinese Remainder theorem to find the unique congruence class $x \pmod n$ satyisfying

$$x \equiv \alpha_i \pmod{p_i^{a_i}}, \quad i = 1, \ldots r$$

and this x will be one of the solutions to (1). All the solutions to (1) are found by considering all possible selections of the α_i. The Chinese Remainder Theorem applies because the indivual moduli $p_i^{a_i}$ are pairwise-coprime since the primes p_i are distinct.

3 for these points

(c) Use the Legendre symbol, the law of quadratic reciprocity and other relevant properties to show that there are no integer solutions to the congruence [6]

$$x^2 \equiv 547 \pmod{631}.$$

(You can use the fact that 547 and 631 are both prime.)

Solution: Solutions x exist if and only if 547 is a quadratic residue modulo 631, i.e. iff the Legendre symbol satisfies $(547|631) = +1$. We develop the Legendre symbol as follows:

$$\begin{aligned}
(547|631) &= -(631|547), \text{ by quad. recip. since } 631 \equiv 547 \equiv 3 \pmod 4 \\
&= -(84|547), \text{cong. prop. and } 631 \equiv 84 \pmod{547} \\
&= -(2|547)^2(3|547)(7|547), \text{multiplicative prop} \\
&= -(547|3)(547|7), \text{quad. recip. and } 547 \equiv 7 \equiv 3 \pmod 4 \\
&= -(1|3)(1|7), \text{xong. prop} \\
&= -1, \text{since } 1 \text{ is always a quad. res.}
\end{aligned}$$

6 marks and six main steps here.

So there are no solutions to the original congruence.

(d) For how many distinct congruence classes $[a]$ modulo 631 will there be integer solutions x to the congruence [2]

$$x^2 \equiv a \pmod{631}?$$

Solution: A solution x exists for this if and only if a is a quadratic residue or $a \equiv 0 \pmod{631}$. By a result from the unit there are $630/2 = 315$ qudratic residues modulo 631. So there are 316 congruence classe modulo 631 for which solutions x exist.

2 needs to cite the $(p-1)/2$ residues result.

End of Section A

SECTION B – Abstract Algebra questions

5. (a) Let G be a non-empty set and $*$ a binary operation on G, i.e. [6]

$$\forall\, g_1, g_2 \in G \quad g_1 * g_2 \in G.$$

State the three extra conditions that the pair $(G, *)$ needs to satisfy in order to be called a **group** and explain their meaning. Illustrate each condition with an example drawn from the group $(\mathbb{R}\backslash\{0\}, \times)$.

(b) The Klein Viergruppe can be thought of as the group $V = \{e, r, h, v\}$, consisting of the four symmetries of a non-square rectangle under the operation of composition. They are the identity e, a rotation r and two reflections h and v.

(i) Write down the Cayley table for the group V. Also write down the Cayley table for the group $\mathbb{Z}_4$, the integers under addition modulo 4. [3]

(ii) From the two Cayley tables point out one feature that shows these two groups have a different structure. [2]

(c) State the definition of a **subgroup**. [2]

(d) Let H and K be subgroups of a group G. Prove that the intersection $H \cap K$ must be a subgroup of G. [3]

(e) Let G be a group and let $Z(G)$ denote the subset of G, called the *centre* of G, defined by [4]

$$Z(G) = \{x \in G \,:\, \text{for all } g \in G \; xg = gx\}\,.$$

Prove that $Z(G)$ forms a subgroup of G.

Solution:

(a) The operation is associative on G, i.e. for all $g, h, k \in G$, $g * (h * k) = (g * h) * k$. This means that no brackets are needed in products of group elements. Multiplication of reals is known to be associative, e.g. $2 \times (3 \times 4) = 24 = (2 \times 3) \times 4$.

There exists an identity element $e \in G$ satisfying for all $g \in G$, $e * g = g * e = g$. When multiplied by any element the identity leaves the other element unchanged. In $(\mathbb{R}\backslash\{0\}, \times)$ the indentity is 1 as for all real x we have $1 \times x = x$.

For all elements $g \in G$ there exists an inverse element $g^{-1} \in G$ satisfying $g*g^{-1} = g^{-1}*g = e$, the identity element of G. In $(\mathbb{R}\backslash\{0\}, \times)$ the inverse elements are the reciprocals, e.g. $2 \times 1/2 = 1$, the identity.

9 marks if all correct, deduct for inaccuracies as appropriate

(b) (i) The Cayley tables are

V	e	r	h	v
e	e	r	h	v
r	r	e	v	h
h	h	v	e	r
v	v	h	r	e

and

$\mathbb{Z}_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

.

3

(ii) In V every element x satisfies $x^2 = e$, i.e. has order 1 or 2. In $\mathbb{Z}_4$ this is not so.

2

(c) A subgroup of a group G is a subset of G that also forms a group using the same operation as in G.

2

(d) Assume that H and K are subgroups of a group G. $e \in H \cap K$ since $e \in H$ and $e \in K$.

1

For any $x \in H \cap K$, $x \in H$ and $x \in K$, therefore $x^{-1} \in H$ and $x^{-1} \in K$ and so $x^{-1} \in H \cap K$.

1

For any $x, y \in H \cap K$, $x, y \in H$ and $x, y \in K$, therefore $xy \in H$ and $xy \in K$ and so $xy \in H \cap K$.

1

(e) $Z(G)$ is non-empty since $e \in Z(G)$.

1

Let $x, y \in Z(G)$ and consider the product xy^{-1} multiplying an element $g \in G$, (associativity used throughout).

$$\begin{aligned} xy^{-1}g &= x(g^{-1}y)^{-1} \\ &= x(yg^{-1})^{-1}, \text{ as } y \in Z(G) \\ &= xgy^{-1} \\ &= gxy^{-1}, \text{ as } x \in Z(G) \end{aligned}$$

Therefore $xy^{-1} \in Z(G)$ and so $Z(G)$ forms a subgroup by the result of part (d). [5]

Or can use the approach from part (d).

3

6. (a) Give the definition of the **subgroup generated by an element** of a group, and the definition of the **order of an element** of a group. [3]

(b) Is every finite abelian group cyclic? Prove or disprove. [3]

(c) Is the symmetric group S_3 abelian? Prove or disprove. [3]

(d) Let $\sigma \in S_n$ be a cycle. Prove that σ can be written as the product of at most $n-1$ transpositions. [3]

(e) Prove that the product of two odd permutations is even. [2]

(f) Let G be a group and let $g \in G$. Define a map $\lambda_g : G \to G$ by $\lambda_g(a) = ga$. Prove that λ_g is a permutation of G. [6]

Solution:

(a) From book.

3

(b) No.

1

For example, $\mathbb{Z}_2 \times \mathbb{Z}_2$ has $(0,0)$ of order 1, and $(0,1)$, $(1,0)$, $(1,1)$ of order 2, but no element of order 4.

2

(c) No

1

For example, $(12)(123) = (23) \neq (13) = (123)(12)$.

2

(d) Let $\sigma = (a_1\, a_2\, \ldots\, a_k)$. Then $k \leq n$, and $\sigma = (a_1\, a_k)(a_1\, a_{k-1}) \cdots (a_1\, a_3)(a_1\, a_2)$, which is the product of $k-1 \leq n-1$ transpositions.

3

(e) If σ and τ are odd, each can be written as the product of an odd number of transpositions. Concatenating these two products, we get $\sigma\tau$ as the product of an even number of transpositions.

2

(f) We need to prove that λ_g is both one-to-one and onto.

2

If $\lambda_g(a) = \lambda_g(b)$, then $ga = gb$, so $a = g^{-1}ga = g^{-1}gb = b$, so λ_g is one-to-one.

2

If $a \in G$, then $\lambda_g(g^{-1}a) = gg^{-1}a = a$, hence λ_g is onto. Therefore λ_g is a permutation of G.

2

SECTION B – Abstract Algebra questions

7. (a) State Lagrange's theorem on the orders of subgroups of a finite group G. [2]

(b) Let H be a subgroup of a finite group G.

(i) State the definition of the **left** and **right cosets** of H in G. [2]

(ii) Let $g_1, g_2 \in G$. Prove that the left-cosets g_1H and g_2H are either equal or disjoint, i.e. [3]

$$g_1H = g_2H \quad \text{or} \quad g_1H \cap g_2H = \emptyset.$$

(iii) Prove that all cosets of H in G contain the same number of elements. [3]

(iv) Then show how parts (ii) and (iii) above can be used to prove Lagrange's theorem. [3]

(c) The dihedral group D_6 is generated by the pair of elements r, s which are subject to the relations $r^6 = e$, $s^2 = e$ and $sr = r^{-1}s$. Consider the subgroup H of D_6 given by

$$H = \{e, r^2, r^4\}.$$

(i) Work out the elements of each left coset of H in D_6. [4]

(ii) Give an example of a subgroup K of D_6 and an element $x \in D_6$ for which [3]

$$xK \neq Kx.$$

Solution:

(a) Anything equivalent to: If G is a finite group and H a subgroup of G then $|H|$ divides $|G|$.

2

(b) (i) The left-coset of H in G with representative $g \in G$ is the subset gH of G defined by

$$gH = \{gh \,:\, h \in H\}.$$

The right-coset of H in G with representative $g \in G$ is the subset Hg of G defined by

$$Hg = \{hg \,:\, h \in H\}.$$

2

(ii) Suppose that $x \in g_1H \cap g_2H$. Therefore there exits $h_1, h_2 \in H$ such that $x = g_1h_1 = g_2h_2$ which implies that $g_1 = g_2h_2h_1^{-1}$ and $g_2 = g_1h_1h_2^{-1}$.

1

Then for all $h \in H$ we have

$$g_1h = g_2h_2h_1^{-1}h \in g_2H,$$

as the product $h_2h_1^{-1}h$ is clearly in H as H is a subgroup. So $g_1H \subseteq g_2H$. Similarly, for all $h \in H$ we have

$$g_2h = g_1h_1h_2^{-1}h \in g_1H.$$

So $g_2H \subseteq g_1H$. Therefore $g_1H = g_2H$. This proves that if the intersection of g_1H and g_2H is non-empty (there is such an x as above) then the two cosets are equal.

So in conclusion any two cosets are either disjoint or equal.

2

(iii) We will show that all cosets of H contain $|H|$ elements by exhibiting the bijection $\phi : H \to gH$ defined by $\phi(h) = gh$.

That this is surjective is clear from the definition of gH.

1

Suppose that $\phi(h_1) = \phi(h_2)$, i.e. $gh_1 = gh_2$. Applying the group cancellation law (multiplying on left by g^{-1}) shows that $h_1 = h_2$. So ϕ is also injective, and hence a bijection. Therefore all cosets contain the same number, $|H|$, of elements.

2

(iv) The collection of cosets of H in G forms a partition of G, meaning every element of G is contained in some coset, for if $g \in G$ then $g \in gH$ as $g = ge \in gH$ as $e \in H$. Also different subsets of the partition are disjoint (from part (ii)).

1

So the total number of elements of G can be found by summing the number of elements in each distinct coset. Part (iii) shows that every coset has the same number of elements, namely $|H|$.

So we get the result of Lagrange's theorem that

$$|G| = [G : H]|H|,$$

where $[G : H]$, the index of H in G is the number of distinct cosets of H in G.

2

(c) (i) The cosets are

$$\begin{aligned} H = r^2H = r^4H &= \{e, r^2, r^4\} \\ rH = r^3H = r^5H &= \{r, r^3, r^5\} \\ sH = r^2sH = r^4sH &= \{e, r^2s, r^4s\} \\ rsH = r^3sH = r^5sH &= \{rs, r^3s, r^5s\}. \end{aligned}$$

4

(ii) An example is $K = \{e, s\}$ and $x = r$. For then we have

$$rK = \{r, rs\} \text{ and } Kr = \{r, r^5s\},$$

which are different since $rs \neq r^5s$.

3

SECTION B – Abstract Algebra questions

8. (a) Give the definition of a **normal subgroup**. [2]

(b) The dihedral group D_6 consists of all products of the two elements r and s, satisfying the relations: [5]

$$r^6 = e,$$
$$s^2 = e,$$
$$srs = r^{-1}.$$

Show that the subgroup $R = \langle r \rangle$ of D_6 generated by r is a normal subgroup of D_6.

(c) Let T be the multiplicative group of non-singular upper triangular 2×2 matrices with entries in $\mathbb{R}$; that is, matrices of the form

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

where $a, b, c \in \mathbb{R}$ and $ac \neq 0$. Let U consist of matrices of the form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

where $x \in \mathbb{R}$.

(i) Prove that U is a subgroup of T. [2]

(ii) Prove that U is abelian. [2]

(iii) Prove that U is normal in T. [3]

(iv) Prove that the factor group T/U is abelian. [3]

(v) Is T normal in the general linear group $GL_2(\mathbb{R})$? Prove or disprove. [3]

Solution:

(a) From book.

2

(b) The order of D_6 is 12 and the order of $R = \{e, r, r^2, \ldots, r^5\}$ is 6, hence there are only two left cosets and two right cosets.

2

One of the cosets is always R, and the other is always $D_6 \setminus R$, the complement of R in D_6, so the left and the right cosets are the same sets. Therefore R is normal.

3

Might also prove the normality condition with an element focused argument, i.e. showing directly that $xR = Rx$ for all $x \in D_6$.

(c) (i) By a theorem from the book, it suffices to show that U contains the identity, and the products and inverses of elements of U. Indeed, we have

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in U,$$
$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} \in U,$$
$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} \in U.$$

2

(ii) Commutativity follows from

$$\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & y\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & x+y\\ 0 & 1\end{pmatrix}$$

and the fact that $x + y = y + x$.

2

(iii) Let

$$g = \begin{pmatrix}a & b\\ 0 & c\end{pmatrix}$$

be an arbitrary element of T. Then for any $x \in \mathbb{R}$,

$$\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix} = \begin{pmatrix}a & ax+b\\ 0 & c\end{pmatrix} = \begin{pmatrix}1 & ax/c\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ 0 & c\end{pmatrix},$$

so $gU \subseteq Ug$; similarly we can show that $Ug \subseteq gU$ and so $gU = Ug$.

3

(iv) With g as above, we can see from (iii) that the coset gU consists of all the matrices from T with diagonal (a, c). Such a coset consists of matrices of the form

$$\begin{pmatrix}a & *\\ 0 & c\end{pmatrix},$$

where the entry $*$ is unspecified. Then we have

$$\begin{pmatrix}a & *\\ 0 & c\end{pmatrix}\begin{pmatrix}a' & *\\ 0 & c'\end{pmatrix} = \begin{pmatrix}aa' & *\\ 0 & cc'\end{pmatrix} = \begin{pmatrix}a' & *\\ 0 & c'\end{pmatrix}\begin{pmatrix}a & *\\ 0 & c\end{pmatrix},$$

so multiplication in T/U is commutative.

3

(v) No. For instance,

$$\begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}^{-1} = \begin{pmatrix}1 & 0\\ -2 & 1\end{pmatrix},$$

however

$$\begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ -2 & 1\end{pmatrix} = \begin{pmatrix}-1 & 1\\ -4 & 3\end{pmatrix} \notin T.$$

Therefore there exists $g \in GL_2(\mathbb{R})$ such that $gTg^{-1} \not\subseteq T$.

3

End of Section B

End OF QUESTIONS