Manchester Metropolitan University

Mock Examination 02
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 the relation is transitive, i.e. [6]

$$(a|b\ \&\ b|c) \Rightarrow a|c.$$

Solution: Let $a, b \in \mathbb{Z}$. We say that a divides b, and write it as $a|b$, if and only if there exists $c \in \mathbb{Z}$ such that

$$b = ac.$$

2

Suppose that $a|b$ and $b|c$, i.e. there exists $r, s \in \mathbb{Z}$ such that

$$b = ra, \quad c = sb.$$

2

Now we can express c as

$$c = sra,$$

which means that $a|c$ by definition.

3

(b) Write down the definition of $\gcd(a, b)$. How is the value of $\gcd(a, b)$ characterised in tewrms of linear combinations of the two integers a and b? [5]

Solution: The greatest common divisor, $\gcd(a, b)$, of integers a and b is the largest integer c that divides a and divides b.

3

If $\gcd(a, b) = c$ then c is also the least positive integer that is a linear combination of a and b.

2

(c) Use the Euclidean Algorithm to calculate $gcd(136, 36)$. Give brief explanations for the main steps of the algorithm and explain why the output produced is the gcd. [4]

Solution: The sequence of integer divisions is

$$\begin{aligned} 136 &= 36 \times 3 + 28, \\ 36 &= 28 \times 1 + 8, \\ 28 &= 8 \times 3 + 4, \\ 8 &= 4 \times 2 + 0. \end{aligned}$$

3

In each integer division $a = bq + r$ the $\gcd$ satisfies $\gcd(a, b) = \gcd(b, r)$. So the $\gcd$ is preserved all the way down the divisions until we have

$$\gcd(136, 36) = \cdots = \gcd(4, 0) = 4.$$

1

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

$$\forall n \geq 1 \quad 8 \,|\, \left(3^{2n} + 7\right).$$

Solution: When $n = 1$ the statement is $8|16$ which is clearly true. Assume that $8|3^{2k} + 7$ for some $k \geq 1$, i.e. $3^{2k} + 7 = 8q$ for some $q \in \mathbb{Z}$. Then

2

$$\begin{aligned} 3^{2(k+1)} + 7 &= 3^{2k+2} + 7 \\ &= 9\left(3^{2k} + 7\right) - 56 \\ &= 8 \times (9q - 7). \text{ by above assumption} \end{aligned}$$

And so we have that $8|3^{2(k+1)} + 7$. So by the principle of induction the result is true for all $n \geq 1$.

3

2. (a) Prove that there are infinitely many prime numbers (Euclid's theorem). State clearly any results about divisibility that you make use of. [10]

Solution:

Suppose there are only a finite number of prime numbers. We could denote them

$$p_1, p_2, p_3, \ldots, p_N.$$

1

Consider the integer M, given by

$$M = p_1 p_2 \ldots p_N + 1.$$

2

By the Fundamental Theorem of Arithmetic (or other results) M is either prime or has a prime factor.

1

Now for each $i = 1, 2, \ldots N$, $M > p_i$, so we conclude that M is not prime.

2

Therefore, it has a prime divisor, p_j say, for some $1 \leq j \leq N$. However, rewriting the definition of M we see that

$$1 = M - p_1 p_2 \ldots p_N.$$

But then $p_j|1$, since $p_j|p_1 \ldots p_N$ and $p_j|M$, i.e. $p_j = \pm 1$. However this is a contradiction since p_j is a prime.

3

So our assumption at the beginning of this proof is false, i.e. there are infinitely many primes as required.

1

(b) What are the possible remainders r left when a prime p is divided by 8 as in [5]

$$p = 8q + r, \quad (0 \leq r < 8)?$$

Hence prove that the integer $p^2 - 1$ is never a prime for any prime $p > 2$.

Solution:

Let $p > 2$ be a prime. Attempting to divide p by 8 will lead to

$$p = 8q + r, \quad r = 1,\ 3,\ 5 \text{ or } 7.$$

The remainders $r = 0, 2, 4,$ or 6 can not occur as they would imply that p is divisible by 2 whereas $p > 2$ is prime.

2

So $p^2 - 1$ is one of

$$p^2 - 1 = (8q + 1)^2 - 1 = 64q^2 + 16q = (8q^2 + 2q) \times 8,$$

or

$$p^2 - 2 = (8q + 3)^2 - 1 = 64q^2 + 16q + 8 = (8q^2 + 2q + 1) \times 8,$$

or

$$p^2 - 2 = (8q + 5)^2 - 1 = 64q^2 + 16q + 24 = (8q^2 + 2q + 3) \times 8,$$

or

$$p^2 - 2 = (8q + 7)^2 - 1 = 64q^2 + 16q + 48 = (8q^2 + 2q + 6) \times 8.$$

In all cases $p^2 - 1$ is divisible by 8 as shown, and so cannot be prime.

3

(c) Prove that if $2^n - 1$ is prime then n is prime. (Hint: Prove the contra-positive). [5]

Solution: The contrapositive of the result in question is the statement: If n is composite then $2^n - 1$ is composite.

1

So assume that n is composite, i.e. we can write $n = rs$ for some $r, s \in \mathbb{Z}$ and $r, s > 1$. We can produce a factorisation for $2^n - 1$ as follows using a standard factorisation for differences of powers,

$$\begin{aligned} 2^n - 1 &= 2^{rs} - 1 \\ &= (2^r)^s - 1^s \\ &= (2^r - 1) \sum_{i=0}^{s-1} (2^r)^{s-1-i}. \end{aligned}$$

2

Is this a genuine factorisation of $2^n - 1$? Yes, both factors are strictly greater than 1 as $r, s > 1$. So this shows that $2^n - 1$ is composite. So we have proved the appropriate contrapositive, so we can conclude that the result in the question is true.

2

SECTION A – Number Theory questions

3. (a) Carefully state the definition of the relation $a \equiv b \pmod{n}$. How does it relate to the remainders produced when a and b are divided by n? [3]

> **Solution:**
>
> Let $a, b, n \in \mathbb{Z}$ with $n \neq 0$. We say that a is congruent to b modulo n, written as $a \equiv b \pmod{n}$ if and only if $n|a-b$.
>
> *2*
>
> When a and b are divided by n we get expressions $a = q_1 n + r$ and $b = q_2 n + s$, where $0 \leq r, s < n$. The relation $a \equiv b \pmod{n}$ is equivalent to $r = s$.
>
> *1*

(b) Suppose that $ac \equiv bc \pmod{m}$ and that $d = \gcd(c, m)$. Prove that [10]

$$a \equiv b \pmod{\frac{m}{d}}.$$

> **Solution:**
>
> If $ac \equiv bc \pmod{m}$ then $m|(a-b)c$, i.e.
>
> $$(a-b)c = qm$$
>
> for some integer q.
>
> *1*
>
> If $\gcd(c, m) = d$ then there exist integers γ, μ such that
>
> $$c = \gamma d, \text{ and } m = \mu d.$$
>
> Moreover, $\gcd(\gamma, \mu) = 1$.
>
> *4*
>
> Then the above equation becomes
>
> $$(a-b)\gamma d = q\mu d,$$
>
> which implies that
>
> $$(a-b)\gamma = q\mu.$$
>
> This shows that $\mu|(a-b)\gamma$, but since $\gcd(\gamma, \mu) = 1$ Euclid's lemma implies that
>
> $$\mu|a-b.$$
>
> This is the required result.
>
> *5*

(c) What is the remainder left when 2013^{2013} is divided by 10? In your solution you should exploit the properties of congruence to avoid as far as possible the direct evaluation of large integers. [7]

> **Solution:**
>
> The remainder r that is left after 2013^{2013} is divided by 10 is the smallest non-negative r

such that

$$2013^{2013} \equiv r \pmod{10}.$$

1

First we replace the base 2013. Note that $2013 \equiv 3 \pmod{10}$. So

$$2013^{2013} \equiv 3^{2013} \pmod{10}.$$

2

Now $\phi(10) = 4$, where ϕ is the Euler totient function. By Euler's theorem we have

$$3^4 \equiv 1 \pmod{10}.$$

1

Note that $2013 = 503 \times 4 + 1$. So we can exploit the properties of congruences as follows (all congruences are modulo 10)

$$\begin{aligned} 3^{2013} &= \left(3^4\right)^{503} \times 3^1, \\ &\equiv 1^{503} \times 3, \\ &\equiv 3. \end{aligned}$$

So a remainder of 3 is left after 2013^{2013} is divided by 10.

3

4. (a) Consider the congruence [7]

$$30x \equiv 18 \pmod{84}.$$

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

Solution: Using the result about linear congruences from the handout we see that $\gcd(30, 84) = 6$ and $6|18$ so there are six solutions to the congruence given by

$$t + 14i, \quad (i = 0, 1, 2, 3, 4, 5)$$

where t is the unique solution $0 \leq t \leq 13$ to the reduced congruence

$$5x \equiv 3 \pmod{14}.$$

2

From the Euclidean algorithm (or simple observation) we see that $5^{-1} \equiv 3 \pmod{14}$ so that

$$t \equiv 3 \times 3 \equiv 9 \pmod{14}.$$

3

So the five solutions to the original congruence are given by

$$x \equiv 9,\ 23,\ 37,\ 51,\ 65,\ 79 \pmod{84}.$$

2

(b) Use the Chinese Remainder Theorem to describe the integers x that satisfy all three of the [7] following congruences simultaneously,

$$\begin{aligned} x &\equiv 2 \pmod{5} \\ x &\equiv 5 \pmod{11} \\ x &\equiv 9 \pmod{13}. \end{aligned}$$

Your final answer should be in the form of a single congruence class for x modulo an appropriate modulus.

Solution: We use the Chinese Remainder theorem from the handout. Firstly the three moduli $m_1 = 5,\ m_2 = 11,\ m_3 = 13$ are pairwise coprime so the theorem applies.

Let $M = 5 \times 11 \times 13 = 715$. Then we have

$$M_1 = 143,\ M_2 = 65,\ M_3 = 55,$$

2

and the multiplicative inverses M_i' of M_i modulo m_i,

$$M_1' = 2,\ M_2' = 10,\ M_3' = 9.$$

3

The solutions x to the system of congruences in the question are all of the integers in the congruence class

$$\begin{aligned} x &\equiv 2M_1M_1' + 5M_2M_2' + 9M_3M_3' \pmod{715} \\ &\equiv 8277 \pmod{715} \\ &\equiv 412 \pmod{715}. \end{aligned}$$

2

(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]

$$x^2 \equiv 503 \pmod{631}.$$

(You can use the fact that 503 and 631 are both prime.)

Solution: Solutions x exist if and only if 503 is a quadratic residue modulo 631, i.e. iff the Legendre symbol satisfies $(503|631) = +1$.

We evaluate the Legendre symbol $(503|631)$ as follows

$$\begin{aligned} (503|631) &= -(631|503) \quad \text{(quad. recip.)} \\ &= -(128|503) \quad (\text{since } 631 \equiv 128 \pmod{503}) \\ &= -(2|503)^7 \quad (\text{since } 128 = 2^7 \text{ using multiplicative prop. of } (\cdot|503)) \\ &= -1 \quad (\text{since } 503 \equiv 7 \equiv -1 \pmod{8} \text{ and known values of } (2|\cdot)) \end{aligned}$$

5

So 503 is not a quadratic residue modulo 631 and there are no solutions to the congruence in question.

1

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 pair $(\mathbb{Z}, +)$.

> **Solution:** The operation is associative on G, i.e. for all $g, h, k \in G$, $g * (h * k) = (g * h) * k$. This is true for addition of integers, e.g. $1 + (2 + 3) = 6 = (1 + 2) + 3$.
>
> *2*
>
> 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 $(\mathbb{Z}, +)$ the identity is the integer 0, e.g. $1 + 0 = 0 + 1 = 1$.
>
> *2*
>
> 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.
>
> *2*

(b) Explain why the pair $(\mathbb{R}, \times)$, consisting of the real numbers and the operation of multiplication does not form a group. What modification is needed to $\mathbb{R}$ so that a group can be formed with the operation $\times$? [2]

> **Solution:** While $(\mathbb{R}, \times)$ satisfies associativity and there is an indtenity element, namely the number 1, it fails to satisfy the existence of inverses property as there is no multitplicative inverse for the number 0 in $\mathbb{R}$. If we omit 0 then we do have a group, i.e. $(\mathbb{R}\backslash\{0\}, \times)$ is a group.
>
> *2*
>
> *1 for 0 not having inverse, 1 for the fix*

(c) Which matrices are elements of the group GL$(n, \mathbb{R})$? Prove that this is a group under the operation of matrix multiplication. Clearly state any properties of matrices that you use. [7]

> **Solution:** GL$(n, \mathbb{R})$ is the group of $n \times n$ matrices with real coefficients and non-zero determinant under the operation of multiplication.
>
> *1*
>
> The determinant satisfies
> $$\det(AB) = \det(A)\det(B).$$
> So if $\det(A)$ and $\det(B)$ are non-zero then so is $\det(AB)$. Therefore GL$(n, \mathbb{R})$ is closed under matrix multiplication.
>
> *2*
>
> Matrix multiplication is known to be associative, i.e. for all $n \times n$ matrices A, B, C,
> $$A(BC) = (AB)C.$$
>
> *1*
>
> The identity element is the similarly named $n \times n$ *identity* matrix $I = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$, which clearly satisfies for all $n \times n$ matrices A, $AI = IA = A$.

1

Lastly, every $n \times n$ matrix A with non-zero determinant has an inverse (w.r.t. mat. mult.) which has determinant $1/\det(A)$ which is also non-zero and hence an element of GL$(n, \mathbb{R})$.

2

(d) Consider the set of 3×3 upper-triangular matrices $H \subset$ GL$(n, \mathbb{R})$ given by [5]

$$H = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \,:\, x, y, z \in \mathbb{R} \right\}.$$

Prove that H forms a subgroup of GL$(n, \mathbb{R})$.

Solution: Note that all matrices in H have determinant equal to 1 so H is indeed a subset of GL$(n, \mathbb{R})$. The identity matrix is clearly an element of H (use $x = y = z = 0$). Associativity holds in H as it holds in GL$(n, \mathbb{R})$. So it just remains to prove that H is closed under matrix multiplication and contains the necessary inverse matrices.

2

Checking closure we find

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+x & b+xc+y \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix} \in H.$$

1

Checking for inverses we find

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x & xz-y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix} \in H.$$

2

6. (a) Suppose that G is a group. State the definition of the terms *subgroup* of G and *order*, $|g|$, of an element of G. [5]

Solution: A subset $H \subseteq G$ forms a subgroup of G if H is itself a group using the same operation of the group G.

2

The order, $|g|$ of an element $g \in G$ is the least positive integer $k \geq 1$ such that $g^k = e$.

3

(b) Let $C_n = \langle a \rangle$ denote the cyclic group of order n generated by an element a and written using multiplicative notation, so that

$$C_n = \{e, a, a^2, a^3, \ldots, a^{n-1}\}.$$

(i) Prove that every subgroup H of C_n is cyclic by proving that $H = \langle a^k \rangle$, where k is the smallest non-negative integer such that $a^k \in H$. [6]

Solution: Let $H \subseteq G$ be a subgroup and k be the least positive integer $k \geq 1$ such that $a^k \in H$. We claim that

$$H = \langle a^k \rangle = \{(a^k)^n \,:\, n \in \mathbb{Z}\}.$$

Suppose on the contrary that there is some element $h = a^m \in H$ such that m is not a multiple of k.

2
For using proof by contradiction

Then there exists $q \in \mathbb{Z}$ such that $m = qk + r$, where $0 < r < k$. Examining this we find

2
integer division with non-zero remainder

$$\begin{aligned} & a^m = a^{qk+r} \\ \Leftrightarrow\ & a^m = (a^k)^q a^r \\ \Leftrightarrow\ & a^r = a^m (a^k)^{-q}. \end{aligned}$$

Note that $a^m, a^k \in H$, therefore $a^r \in H$. But this contradicts the choice of k as the smallest positive exponent such that $a^k \in H$.

2

So we conclude that $H = \langle a^k \rangle$ as required.

(ii) Prove that $a^m = e$ if and only if $n|m$, i.e. n divides m. [3]

Solution: Suppose on the contrary that $a^m = e$ and m is not a multiple of n. Then like in the previous part there exists integers q, r such that $m = nq + r$ and $0 < r < n$.

1

Then

$$\begin{aligned} e = a^m &= a^{nq+r} \\ &= (a^n)^q a^r \\ &= a^r, \text{ since } a^n = e. \end{aligned}$$

But this contradicts the fact that $|a| = n$, i.e. n is the least such positive exponent of a giving the identity. So any such exponent m must be a multiple of n.

2

(iii) If $b = a^r$ then prove that the order of b in C_n is n/d where $d = \gcd(r, n)$. [3]

Solution: Let $b = a^r$. $|b|$ is the least positive m such that $b^m = e$, i.e. $a^{rm} = e$. By part (ii) this is the least m such that n divides rm,

2

or equivalently, the least m such that n/d divides mr/d. Since n/d is coprime to r/d this is equivalent to the least m such that n/d divides m. The least such m is clearly n/d itself. So we conclude that $|b| = n/d$.

1

(iv) Illustrate these results by determining the elements of *all* the subgroups of the cyclic group, $C_{20} = \langle a \rangle$, the cyclic group of order 20. [3]

Solution: Putting the results of the previous parts together, subgroups of C_{20} are all cyclic and are generated by a^m where m is a divisor of 20. The subgroups are

$$
\begin{aligned}
\langle e\rangle &= \{e\}\\
\langle a^{10}\rangle &= \{e, a^{10}\}\\
\langle a^{5}\rangle &= \{e, a^5, a^{10}, a^{15}\}\\
\langle a^{4}\rangle &= \{e, a^4, a^8, a^{12}, a^{16}\}\\
\langle a^{2}\rangle &= \{e, a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}, a^{18}\}\\
\langle a\rangle &= C_{20}
\end{aligned}
$$

3
partial credit if some of these present

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]

Solution: See solutions to mock 01.

(c) Suppose that G is a group of prime order. Use Lagrange's theorem to prove that G is cyclic. [7]

Solution: Let G be a group with $|G| = p$, where p is prime. Since $p \geq 2$ there is an element $g \in G$ with $g \neq e$.

2

The cyclic subgroup $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ generated by g is a subgroup of G and so $|\langle g \rangle|$ divides p. Since p is prime $|\langle g \rangle| = 1$ or p.

3

But since $g \neq e$, $\langle g \rangle$ contains at least the two elements e and g. Therefore $|\langle g \rangle| = p$, i.e. $\langle g \rangle = G$ and thus G is cyclic.

2

8. (a) Define what is meant by a *normal subgroup* of a group G. [2]

Solution: A subgroup H of a group G is normal in G if left and right cosets represented by the same element are equal, i.e. for all $g \in G$, $gH = Hg$.

2

(b) The dihedral group D_n, the group of symmetries of a regular polygon with n sides, is generated by two elements r, a rotation, and s, a reflection. These are subject to the relations $r^n = e, s^2 = e$ and $sr = r^{-1}s$. The $2n$ elements of D_n can be expressed in the standard form $r^i s^j$, where $0 \leq i \leq n-1$ and $j = 0, 1$.

(i) Prove that $H = \{e, r^3\}$ is a normal subgroup of D_6. [3]

Solution: Firstly, note that r^3 is its own inverse as $r^3 r^3 = r^6 = e$. The non-identity element r^3 in H actually commutes with all elements of D_6, as

$$\begin{aligned} r^i s^j r^3 &= r^i r^{-3} s^j, \text{ repeated application of } sr = r^{-1}s \\ &= r^{i-3} s^j, \text{ exponent rules} \\ &= r^{-3} r^i s^j, \text{ exponent rules} \\ &= r^3 r^i s^j, \text{ as } r^3 \text{ is self-inverse.} \end{aligned}$$

Since each element of H commutes with all elements of D_6 it is true that $xH = Hx$ for every $x \in D_6$.

(ii) What will be the order of the factor group D_6/H? [1]

Solution: By Lagrange's theorem the order of D_6/H is $|D_6|/|H| = 12/2 = 6$.

(iii) Determine the elements of each of the left-cosets of H in D_6. [4]

Solution: The cosets are

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

4
Partial credit for partial correctness

(iv) Assign suitable labels to the cosets and construct a Cayley table for the factor group D_6/H. [4]

Solution: Using the labelling $e = H$, $\rho_1 = rH$, $\rho_2 = r^2H$, $\sigma_1 = sH$, $\sigma_2 = rsH$, $\sigma_3 = r^2sH$, the Cayley table for D_6/H is

	e	ρ_1	ρ_2	σ_1	σ_2	σ_3
e	e	ρ_1	ρ_2	σ_1	σ_2	σ_3
ρ_1	ρ_1	ρ_2	e	σ_2	σ_3	σ_1
ρ_2	ρ_2	e	ρ_1	σ_3	σ_1	σ_2
σ_1	σ_1	σ_3	σ_2	e	ρ_2	ρ_1
σ_2	σ_2	σ_1	σ_3	ρ_1	e	ρ_2
σ_3	σ_3	σ_2	σ_1	ρ_2	ρ_1	e

4

(v) Use your Cayley table to explain why the factor group D_6/H is isomorphic to another dihedral group D_n. [4]

Solution: From the Cayley table we can see that D_6/H matches the definition of D_3 in the questions with $\rho_1 = r$, $\sigma_1 = s$ and the table verifies that

$$sr = \sigma_1\rho_1 = \sigma_3 = \rho_2\sigma_1 = r^{-1}s.$$

So D_6/H is isomorphic to D_3 under the isomorphism $\phi : D_6/H \to D_3$ defined by

$$\begin{aligned} e &\mapsto e \\ \rho_1 &\mapsto r \\ \rho_2 &\mapsto r^2 \\ \sigma_1 &\mapsto s \\ \sigma_2 &\mapsto rs \\ \sigma_3 &\mapsto r^2s \end{aligned}$$

4

(c) Suppose that H and K are normal subgroups of a group G and that $H \cap K = \{e\}$. By carefully considering the commutator $hkh^{-1}k^{-1}$ prove that elements of H and K commute with one another, i.e. [4]

$$\forall\, h \in H\ \forall\, k \in K \quad hk = kh.$$

Solution: First note that an equivalent condition defining a normal subgroup H of G is that for all $g \in G$ and for all $h \in H$, $ghg^{-1} \in H$. Using the principle of associativity we can view the commutator $hkh^{-1}k^{-1}$ as

$$hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K,$$

since the product on the right is a product of elements of K. On the other hand we can view the commutator as

$$hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H,$$

since the product on the right is a product of elements of H.

3

So the commutator is an element of the intersection of H and K. But if this intersection consists of just the identity e then every for every $h \in H$ and $k \in K$, $hkh^{-1}k^{-1} = e$, i.e. $hk = kh$, as required.

1

End of Section B

End OF QUESTIONS