INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

Stamp / Signature of the Invigilator

EXAMINATION (End Semester)										**SEMESTER (Autumn)**			
Roll Number										**Section**		**Name**	
Subject Number	**C**	**S**	**2**	**1**	**0**	**0**	**1**	**Subject Name**		***Discrete Structures***			
Department / Center of the Student											**Additional sheets**		

Important Instructions and Guidelines for Students

1. You must occupy your seat as per the Examination Schedule/Sitting Plan.
2. Do not keep mobile phones or any similar electronic gadgets with you even in the switched off mode.
3. Loose papers, class notes, books or any such materials must not be in your possession, even if they are irrelevant to the subject you are taking examination.
4. Data book, codes, graph papers, relevant standard tables/charts or any other materials are allowed only when instructed by the paper-setter.
5. Use of instrument box, pencil box and non-programmable calculator is allowed during the examination. However, exchange of these items or any other papers (including question papers) is not permitted.
6. Write on both sides of the answer script and do not tear off any page. **Use last page(s) of the answer script for rough work.** Report to the invigilator if the answer script has torn or distorted page(s).
7. It is your responsibility to ensure that you have signed the Attendance Sheet. Keep your Admit Card/Identity Card on the desk for checking by the invigilator.
8. You may leave the examination hall for wash room or for drinking water for a very short period. Record your absence from the Examination Hall in the register provided. Smoking and the consumption of any kind of beverages are strictly prohibited inside the Examination Hall.
9. Do not leave the Examination Hall without submitting your answer script to the invigilator. **In any case, you are not allowed to take away the answer script with you.** After the completion of the examination, do not leave the seat until the invigilators collect all the answer scripts.
10. During the examination, either inside or outside the Examination Hall, gathering information from any kind of sources or exchanging information with others or any such attempt will be treated as '**unfair means**'. Do not adopt unfair means and do not indulge in unseemly behavior.

Violation of any of the above instructions may lead to severe punishment.

Signature of the Student

To be filled in by the examiner

Question Number	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Total**
Marks Obtained											

Marks obtained (in words)	**Signature of the Examiner**	**Signature of the Scrutineer**

CS21001 Discrete Structures, Autumn 2019–2020

End-Semester Test

27–November–2019 NR 221/222/321/322, 09:00am–12:00pm Maximum marks: 80

Instructions

- Write your answers in the question paper itself. Be brief and precise. Answer all questions.
- Write the answers only in the respective spaces provided. The blank pages at the end may be used for rough work.
- If you use any theorem/result/formula covered in the class, just mention it, do not elaborate.
- Write all the proofs in mathematically precise language. Unclear and/or dubious statements would be severely penalized.
- Common notations:

$$
\begin{aligned}
\mathbb{N} &= \text{The set of natural numbers } = \{1,2,3,\ldots\} \\
\mathbb{N}_0 &= \text{The set of non-negative integers } = \{0,1,2,3,\ldots\} \\
\mathbb{Z} &= \text{The set of integers } = \{\ldots,-3,-2,-1,0,1,2,3,\ldots\} \\
\mathbb{Q} &= \text{The set of rational numbers } = \left\{\frac{a}{b} \mid a \in \mathbb{Z},\ b \in \mathbb{N}\right\} \\
\mathbb{R} &= \text{The set of real numbers} \\
\mathbb{C} &= \text{The set of complex numbers} \\
\mathscr{P}(A) &= \text{The power set of } A \text{ (also denoted as } 2^A) \\
(a,b) &= \text{The open interval } \{x \in \mathbb{R} \mid a < x < b\} \\
[a,b] &= \text{The closed interval } \{x \in \mathbb{R} \mid a \leqslant x \leqslant b\} \\
\lfloor x \rfloor &= \text{The floor of } x \\
\lceil x \rceil &= \text{The ceiling of } x
\end{aligned}
$$

Do not write anything on this page.

Questions start from the next page.

1. You are given n sticks. The length of each stick (a real number) is more than one, but no more than 55, and these lengths need not be distinct from one another. Prove that you can choose three of the given sticks to form a triangle. The triangle should be non-degenerate, that is, its three corners must be non-collinear. **(8)**

Solution Let the stick lengths in ascending order be $l_1, l_2, \ldots, l_{10}$. By the given conditions,

$$1 < l_1 \leqslant l_2 \leqslant l_3 \leqslant \cdots \leqslant l_{10} \leqslant 55.$$

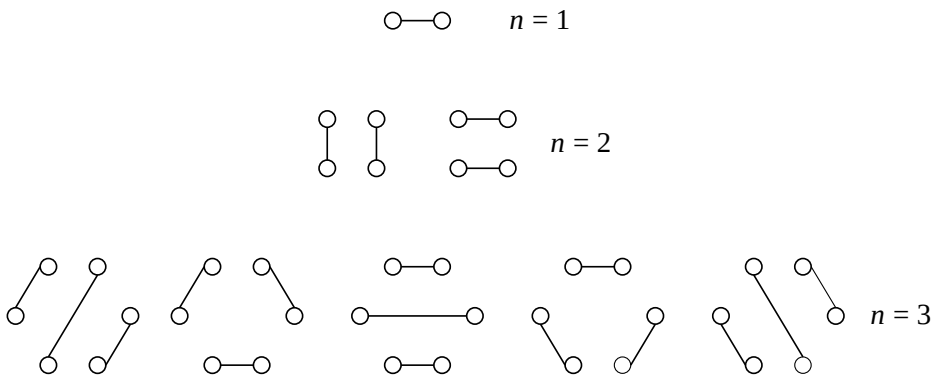
Suppose that no non-degenerate triangle can be formed by any three of the sticks. This in particular implies that

$$\begin{aligned}
l_3 &\geqslant l_2 + l_1 > 1 + 1 = 2, \\
l_4 &\geqslant l_3 + l_2 > 2 + 1 = 3, \\
l_5 &\geqslant l_4 + l_3 > 3 + 2 = 5, \\
l_6 &\geqslant l_5 + l_4 > 5 + 3 = 8, \\
l_7 &\geqslant l_6 + l_5 > 8 + 5 = 13, \\
l_8 &\geqslant l_7 + l_6 > 13 + 8 = 21, \\
l_9 &\geqslant l_8 + l_7 > 21 + 13 = 34, \\
l_{10} &\geqslant l_9 + l_8 > 34 + 21 = 55.
\end{aligned}$$

This contradicts the fact that $l_{10} \leqslant 55$.

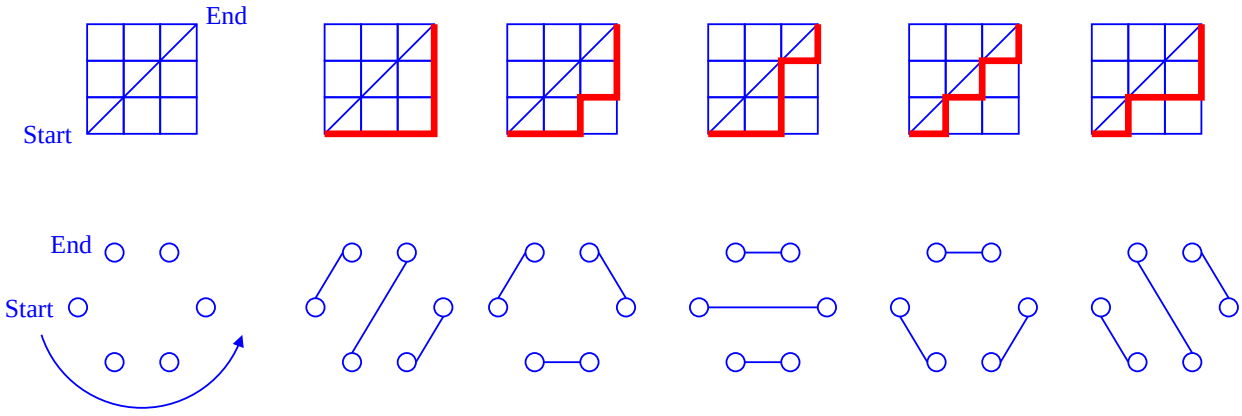
This question has a serious typo. Here, n should be ten. The proposition is true for all $n \geqslant 10$, but not for $n < 10$. This question will not be evaluated, that is, the total will be in $80 - 8 = 72$.

2. $2n$ persons are seated around a circular table. Each of them simultaneously shakes hands with another person at the table in such a way that the arms do not cross each other. The following figure shows the possibilities for $n = 1, 2, 3$.



In how many ways can such handshaking be done by the $2n$ persons? **(10)**

Solution The answer is the n-th Catalan number C_n. In order see why, let us establish a one-to-one correspondence between (1) all paths in a grid from $(0,0)$ to (n,n), that do not cross the main diagonal, and (2) all the possibilities of handshakes. Let us fix one position on the table as the start position and one direction (like counterclockwise). Given a path in the grid, we proceed as follows. When we find a horizontal move, the current person extends his hand. When we find a vertical move, the current person accepts the handshake invitation from the last person who extended his hand (and has not yet been responded to). The following figure demonstrates this construction.



This construction is reversible, and thereby establishes a bijection between the set of allowed paths and the set of allowed handshake patterns.

3. Let l_n be the number of lines printed by the call $f(n)$ for some integer $n \geqslant 0$.

```
void f ( int n )
{
    int i, j;

    printf("Hi\n");

    if (n == 0) return;
    for (i=0; i<=n-1; ++i)
        for (j=0; j<=i; ++j)
            f(j);
}
```

(a) Let $L(x) = l_0 + l_1 x + l_2 x^2 + \cdots + l_n x^n + \cdots$ be the generating function of the sequence $l_0, l_1, l_2, \ldots$. Prove that $L(x) = \dfrac{1-x}{1-3x+x^2}$. **(6)**

Solution The function gives the following recurrence relation for the sequence.

$$\begin{aligned} l_0 &= 1, \\ l_n &= 1 + l_{n-1} + 2l_{n-2} + 3l_{n-3} + \cdots + nl_0 \quad \text{for } n \geqslant 1. \end{aligned}$$

Therefore we have

$$\begin{aligned} L(x) &= l_0 + \sum_{n\geqslant 1} l_n x^n \\ &= 1 + \sum_{n\geqslant 1} (1 + l_{n-1} + 2l_{n-2} + 3l_{n-3} + \cdots + nl_0) x^n \\ &= \sum_{n\geqslant 0} x^n + \sum_{n\geqslant 1} (l_{n-1} + 2l_{n-2} + 3l_{n-3} + \cdots + nl_0) x^n \\ &= \frac{1}{1-x} + x \sum_{n\geqslant 0} (l_n + 2l_{n-1} + 3l_{n-2} + \cdots + (n+1)l_0) x^n \\ &= \frac{1}{1-x} + \frac{xL(x)}{(1-x)^2}. \end{aligned}$$

It follows that

$$(1-x)^2 L(x) = 1 - x + xL(x),$$

that is,

$$L(x) = \frac{1-x}{1-3x+x^2}.$$

(b) Derive an explicit formula for l_n (valid for all $n \geqslant 0$) from the generating function $L(x)$. **(6)**

Solution We have

$$\begin{aligned} L(x) &= \frac{1-x}{1-3x+x^2} \\ &= \frac{1-x}{\left(1-\left(\frac{3+\sqrt{5}}{2}\right)x\right)\left(1-\left(\frac{3-\sqrt{5}}{2}\right)x\right)} \\ &= \frac{A}{1-\left(\frac{3+\sqrt{5}}{2}\right)x} + \frac{B}{1-\left(\frac{3-\sqrt{5}}{2}\right)x}. \end{aligned}$$

Solving for A and B (show the steps) gives

$$A = \frac{\sqrt{5}+1}{2\sqrt{5}}, \qquad B = \frac{\sqrt{5}-1}{2\sqrt{5}}.$$

Therefore

$$l_n = \left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right)\left(\frac{3+\sqrt{5}}{2}\right)^n + \left(\frac{\sqrt{5}-1}{2\sqrt{5}}\right)\left(\frac{3-\sqrt{5}}{2}\right)^n \quad \text{for all } n \geqslant 0.$$

4. Solve the following recurrence relation with the given initial condition. Take $n \geqslant 2$. **(10)**

$$\begin{aligned} a_2 &= 1, \\ a_n &= (n-2)a_{n-1} + (n-1)! \text{ for } n \geqslant 3. \end{aligned}$$

Solution The substitution $b_n = a_n/n!$ for $n \geqslant 2$ gives

$$\begin{aligned} b_2 &= \frac{1}{2}, \\ b_n &= \left(\frac{n-2}{n}\right) b_{n-1} + \frac{1}{n} \text{ for } n \geqslant 3. \end{aligned}$$

Let us now repeatedly unfold the recurrence to get

$$\begin{aligned} b_n &= \left(\frac{n-2}{n}\right) b_{n-1} + \frac{1}{n} \\ &= \left(\frac{(n-2)(n-3)}{n(n-1)}\right) b_{n-2} + \frac{n-2}{n(n-1)} + \frac{1}{n} \\ &= \left(\frac{(n-2)(n-3)(n-4)}{n(n-1)(n-2)}\right) b_{n-3} + \frac{(n-2)(n-3)}{n(n-1)(n-2)} + \frac{n-2}{n(n-1)} + \frac{1}{n} \\ &= \left(\frac{(n-3)(n-4)}{n(n-1)}\right) b_{n-3} + \frac{n-3}{n(n-1)} + \frac{n-2}{n(n-1)} + \frac{1}{n} \\ &= \left(\frac{(n-3)(n-4)(n-5)}{n(n-1)(n-3)}\right) b_{n-4} + \frac{(n-3)(n-4)}{n(n-1)(n-3)} + \frac{n-3}{n(n-1)} + \frac{n-2}{n(n-1)} + \frac{1}{n} \\ &= \left(\frac{(n-4)(n-5)}{n(n-1)}\right) b_{n-4} + \frac{(n-4)}{n(n-1)} + \frac{n-3}{n(n-1)} + \frac{n-2}{n(n-1)} + \frac{1}{n} \\ &= \cdots \\ &= \left(\frac{2 \times 1}{n(n-1)}\right) b_2 + \left(\frac{2+3+4+\cdots+(n-2)+(n-1)}{n(n-1)}\right) \\ &= \frac{1}{n(n-1)} + \left(\frac{\frac{n(n-1)}{2} - 1}{n(n-1)}\right) \\ &= \frac{1}{2}. \end{aligned}$$

It then follows that

$$a_n = n! b_n = \frac{n!}{2} \text{ for all } n \geqslant 2.$$

5. Consider the following set of 2×2 matrices with real entries: $\mathbb{A} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \, a, b \in \mathbb{R} \right\}$.

(a) Prove that $\mathbb{A}$ is a commutative ring with identity. **(5)**

Solution Since $\mathbb{A}$ is a subset of the ring of 2×2 matrices with real entries, it suffices to show closure under addition, multiplication, and additive inverse in order to prove that $\mathbb{A}$ is a ring.

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} (a+c) & (b+d) \\ -(b+d) & (a+c) \end{pmatrix}.$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} (ac-bd) & (ad+bc) \\ -(ad+bc) & (ac-bd) \end{pmatrix}.$$

$$-\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} (-a) & (-b) \\ -(-b) & (-a) \end{pmatrix}.$$

For commutativity, note that

$$\begin{aligned} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} &= \begin{pmatrix} (ac-bd) & (ad+bc) \\ -(ad+bc) & (ac-bd) \end{pmatrix} \\ &= \begin{pmatrix} (ca-db) & (da+cb) \\ -(da+cb) & (ca-db) \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix}. \end{aligned}$$

Finally, the 2×2 identity matrix is in $\mathbb{A}$.

(b) Prove that $\mathbb{A}$ is isomorphic to the ring $\mathbb{C}$ of complex numbers. **(5)**

Solution Define the map $f : \mathbb{A} \to \mathbb{C}$ as

$$f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = a + \mathrm{i}b.$$

We have

$$\begin{aligned} f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) &= f\left(\begin{pmatrix} (a+c) & (b+d) \\ -(b+d) & (a+c) \end{pmatrix}\right) = (a+c) + \mathrm{i}(b+d) \\ &= (a+\mathrm{i}b) + (c+\mathrm{i}d) = f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) + f\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right), \end{aligned}$$

and

$$\begin{aligned} f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) &= f\left(\begin{pmatrix} (ac-bd) & (ad+bc) \\ -(ad+bc) & (ac-bd) \end{pmatrix}\right) = (ac-bd) + \mathrm{i}(ad+bc) \\ &= (a+\mathrm{i}b)(c+\mathrm{i}d) = f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) f\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right). \end{aligned}$$

Therefore f is a ring homomorphism. Clearly, f is surjective. Finally,

$$f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = f\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right)$$

implies that $a + \mathrm{i}b = c + \mathrm{i}d$, that is, $a = c$ and $b = d$, that is,

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}.$$

So f is injective too.

6. Let R be a ring, and I an ideal of R. Define the *radical* of I as

$$\operatorname{rad}(I) = \left\{ a \in R \;\middle|\; a^n \in I \text{ for some } n \in \mathbb{N} \right\}.$$

(a) If R is commutative, prove that $\operatorname{rad}(I)$ is an ideal of R. **(5)**

Solution Let $a, b \in \operatorname{rad}(I)$. Then, $a^m \in I$ and $b^n \in I$ for some $m, n \in \mathbb{N}$. Since R is commutative, the binomial theorem gives

$$(a-b)^{m+n} = \sum_{\substack{i,j=0 \\ i+j=m+n}}^{m+n} \binom{m+n}{i} (-1)^j a^i b^j.$$

For each i, j in the sum, either $i \geqslant m$ or $j \geqslant n$, that is, either $a^i \in I$ or $b^j \in I$. Therefore each summand in the above sum is in I (since I is closed under multiplication by any element of R). It follows that $(a-b)^{m+n} \in I$, that is, $a - b \in \operatorname{rad}(I)$. Now, take any $a \in \operatorname{rad}(I)$ and $r \in R$. We have $a^m \in I$ for some $m \in \mathbb{N}$, so by commutativity, $(ra)^m = r^m a^m \in I$, that is, $ra \in \operatorname{rad}(I)$.

(b) Demonstrate by an example that if R is not commutative, then $\mathrm{rad}(I)$ is not necessarily an ideal of R. **(5)**

Solution Consider the ring R of all 2×2 matrices with real entries, and take

$$I = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}.$$

Clearly, I is an ideal of R (the zero ideal). Now, consider the two matrices

$$A = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}.$$

It is easy to see that both A^2 and B^2 are the zero matrix, so $A, B \in \mathrm{rad}(I)$. But

$$A - B = \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}$$

is of determinant $4 \neq 0$, that is, $A - B$ is invertible, so $(A-B)^n$ cannot be the zero matrix for any $n \in \mathbb{N}$.

7. Let p be an odd prime. An element $a \in \mathbb{Z}_p^*$ is called a *quadratic residue* modulo p if $a \equiv b^2 \pmod{p}$ for some $b \in \mathbb{Z}_p^*$. Otherwise, a is called a *quadratic non-residue* modulo p. Let QR_p and QNR_p respectively denote the set of all quadratic residues and the set of all quadratic non-residues modulo p. For example, for $p = 11$, we have $1^2 \equiv 10^2 \equiv 1 \pmod{11}$, $2^2 \equiv 9^2 \equiv 4 \pmod{11}$, $3^2 \equiv 8^2 \equiv 9 \pmod{11}$, $4^2 \equiv 7^2 \equiv 5 \pmod{11}$, and $5^2 \equiv 6^2 \equiv 3 \pmod{11}$. Therefore $\mathrm{QR}_{11} = \{1,3,4,5,9\}$, and so $\mathrm{QNR}_{11} = \mathbb{Z}_{11}^* \setminus \mathrm{QR}_{11} = \{2,6,7,8,10\}$.

(a) Prove that QR_p is a subgroup of the multiplicative group $\mathbb{Z}_p^*$. What is the order of QR_p? **(2 + 2)**

Solution Since QR_p is a finite set, it suffices to show that it is closed under multiplication. Let $a_1, a_2 \in \mathrm{QR}_p$, that is, $a_1 \equiv b_1^2 \pmod{p}$ and $a_2 \equiv b_2^2 \pmod{p}$ for some $b_1, b_2 \in \mathbb{Z}_p^*$. But then, $a_1 a_2 \equiv b_1^2 b_2^2 \equiv (b_1 b_2)^2 \pmod{p}$. Since $b_1 b_2 \in \mathbb{Z}_p^*$, it follows that $a_1 a_2 \in \mathrm{QR}_p$.

Since square-roots of each element in QR_p occur in pairs, we have $|\mathrm{QR}_p| = \frac{1}{2}|\mathbb{Z}_p^*| = \frac{p-1}{2}$.

(b) Let $p \geqslant 5$. Prove that the sum of the elements of QNR_p is a multiple of p. **(6)**

Solution Let $s = \sum_{a \in \mathbb{Z}_p^*} a$, $s_1 = \sum_{a \in \mathrm{QR}_p} a$, and $s_2 = \sum_{a \in \mathrm{QNR}_p} a$. Clearly, $s = s_1 + s_2$. Therefore it suffices to show that both s and s_1 are multiples of p. We have

$$s = 1 + 2 + \cdots + (p-1) = \frac{p(p-1)}{2}.$$

Since p is an odd prime, $(p-1)/2$ is an integer, so $s \equiv 0 \pmod{p}$. The quadratic residues modulo p are $i^2 \equiv (p-i)^2 \pmod{p}$ for $i = 1, 2, \ldots, (p-1)/2$. It follows that

$$s_1 \equiv \frac{1}{2}\left(1^2 + 2^2 + 3^2 + \cdots + (p-1)^2\right) \equiv \frac{p(p-1)(2p-1)}{12} \pmod{p}.$$

Now, $(p-1)(2p-1)/12$ is not necessarily an integer. However, since $p \neq 2, 3$, the inverse of 12 modulo p exists, implying that $s_1 \equiv 0 \pmod{p}$.

8. Let G be a multiplicative group.

(a) Prove that if $(ab)^2 = a^2b^2$ for all $a, b \in G$, then G is abelian. **(5)**

Solution Take any two elements $a, b \in G$. Since $(ab)^2 = a^2b^2$, we have

$$e = (ab)^{-1}(ab)^2(ab)^{-1} = (b^{-1}a^{-1})(a^2b^2)(b^{-1}a^{-1}) = b^{-1}aba^{-1}.$$

This in turn implies that

$$ba = bea = b(b^{-1}aba^{-1})a = (bb^{-1})ab(a^{-1}a) = ab.$$

(b) Define a relation $\sim$ on G as $a \sim b$ if and only if $\langle a \rangle = \langle b \rangle$ (that is, a and b generate the same subgroup of G). It is easy to see that $\sim$ is an equivalence relation on G (you do not have to show this). Prove that each equivalence class of $\sim$ is finite. **(5)**

Solution Take any $a \in G$. Since $\langle a \rangle$ is a cyclic group, we consider two possibilities.

Case 1: $\text{ord}(a) = \infty$.

In this case, $\langle a \rangle \cong (\mathbb{Z}, +)$. But $\mathbb{Z}$ has only two generators ± 1, so $[a] = \{a, a^{-1}\}$, that is, $|[a]| = 2$.

Case 2: $\text{ord}(a) = n$ is finite.

In this case, $\langle a \rangle \cong (\mathbb{Z}_n, +)$. Since $\mathbb{Z}_n$ has $\phi(n)$ generators, it follows that $|[a]| = \phi(n)$.