COL202 Tutorial

1. Recall the proof of the fact that there are infinitely many prime numbers. (If you have never seen it, give it a shot.) Observe that except for 2, all other primes are either of the form $4k+1$ or $4k+3$ for some integer k. Prove that there exist infinitely many primes of the form $4k+3$ for some integer k. (You may use the basic results of modular arithmetic without proving them.)

2. Consider a party of 10 people where some pairs of persons greet each other by fist bumps. Prove that one of the following statements is necessarily true.

   (a) There exist 4 people all of whom give fist bumps to one another.

   (b) There exist 3 people no two of whom give fist bumps to each other.

3. Consider a party of n people where each pair of persons greets in one of three ways: fist bump, high five, and handshake. Determine a small enough value of n that ensures that there are three people who greet one another in the same way.

4. Using the standard principle of mathematical induction, prove that the following variant is also valid.
   Claim: Suppose P is a proposition on $\mathbb{N} \times \mathbb{N}$ such that.

   - $P(1,1)$ is true.
   - For all $m \in \mathbb{N}$ and $m > 1$, $P(m-1,1) \Rightarrow P(m,1)$.
   - For all $m, n \in \mathbb{N}$ and $n > 1$, $P(m,n-1) \Rightarrow P(m,n)$.

   Then $P(m,n)$ is true for all $(m,n) \in \mathbb{N} \times \mathbb{N}$.

5. Find the mistake in the proof given below, if any.
   Claim: $\lim_{x\to 0} \frac{\sin x}{x} = 1$.
   Proof: $\sin 0 = 0$, so if we substitute $x = 0$ in the expression $\frac{\sin x}{x}$, it takes the $0/0$ indeterminate form. We also have
   $$\frac{d}{dx} \sin x = \cos x, \text{ and } \frac{d}{dx} x = 1.$$
   Therefore, by l'Hôpital's rule,
   $$\lim_{x\to 0} \frac{\sin x}{x} = \lim_{x\to 0} \frac{\cos x}{1} = \frac{\cos 0}{1} = 1.$$

6. Prove that the Principle of Mathematical Induction is equivalent to the Well-Ordering Principle, that is, show that if any one of them is taken as an axiom, the other can be proven.

7. A group of an odd number of friends gathers to play Holi, and everybody stands in such a way that the $n(n-1)/2$ pairwise distances between them are all distinct. Then every person throws color at the person who is standing closest to them. Prove that, necessarily, there there exists at least one person who stays clean. Is the claim necessarily true if the number of people is even? Is the claim necessarily true for an odd-sized group if every person throws color at their best friend instead?

8. Use the well-ordering principle to prove the following fact (which you might know already). For every $x, y \in \mathbb{Z}$, there exist $a, b \in \mathbb{Z}$ such that $\gcd(x,y) = ax + by$.

9. Formally, we define a set S to be *infinite* if there is no injection from S to the set $\{1, 2, \ldots, n\}$ for any $n \in \mathbb{N}$. Prove rigorously that if S is an infinite set, then for every $n \in \mathbb{N}$, there exists an injection from $\{1, 2, \ldots, n\}$ to S. (This is a special case of the following more general claim that we mentioned in class without proof: if A and B are non-empty set then there exists an injection from A to B or an injection from B to A.)

10. Prove the following claims about infinite sets.

    (a) If a set S is infinite, then there exists an injection from $\mathbb{N}$ to S.

    (b) If there exists an injection from $\mathbb{N}$ to a set S, then S is infinite.

    (c) If a set S is infinite, then there exists an injection from S to some strict subset of S.

    (d) If there exists an injection from a set S to some strict subset of S, then S is infinite.

    Write the proofs in an appropriate order so that you can take help of the earlier proven claims in proving any claim, if necessary.

11. Prove that if A and B are countable sets, then $A \cup B$ and $A \times B$ are both countable. Hence, prove that for every $n \in \mathbb{N}$, if $A_1, \ldots, A_n$ are countable sets, then $A_1 \cup \cdots \cup A_n$ and $A_1 \times \cdots \times A_n$ are both countable.

12. Determine whether each of the following statements is true or false, and prove your claim.

    (a) If A and B are uncountable sets, then $A \cup B$ is necessarily uncountable.

    (b) If A and B are uncountable sets, then $A \cap B$ is necessarily uncountable.

    (c) If A and B are uncountable sets, then $A \setminus B$ is necessarily uncountable.

    (d) If A and B are uncountable sets, then $A \times B$ is necessarily uncountable.

    (e) If A is an uncountable set and B is a countable set, then $A \setminus B$ is necessarily uncountable.

13. Let $L \subseteq \mathbb{N}$ and let P be a program written in your favorite programming language that accepts an integer as input, and outputs a string. We say that P *recognises* L if it satisfies the following properties.

    (a) For every $n \in \mathbb{N}$, if $n \in L$, then P on input n prints 'Yes' and halts.

    (b) For every $n \in \mathbb{N}$, if $n \notin L$, then P on input n does anything except printing 'Yes' and halting (eg. print some junk and halt, or print 'Yes' but not halt, and so on).

    Prove that there exists a set $L \subseteq \mathbb{N}$ for which there does not exist a program P that recognises L. As a challenge, fix some programming language and construct an explicit L which satisfies this property.

14. Let S be an arbitrary set. Prove that there does not exist an injection from 2^S to S. (We did the particular case where $S = \mathbb{N}$ in class. This general statement is known as Cantor's theorem. You should easily find its proof on the Internet, but you should not do this and try to write the proof on your own instead, referring only to the lecture.)

15. Prove the handshake lemma by mathematical induction.

16. The degree sequence of a graph $G = (V, E)$ is a sorted array containing $|V|$ numbers: the degrees of all vertices of G. If two graphs are isomorphic, are their degree sequences necessarily equal? If the degree sequences of two graphs are equal, are the graphs necessarily isomorphic?

17. Determine all automorphisms of the following graphs.

    (a) The 5-cycle graph, where

    $$V = \{v_0, v_1, v_2, v_3, v_4\}, \text{ and } E = \{\{v_0, v_1\}, \{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}, \{v_4, v_0\}\}.$$

    (b) The cube graph, where

    $$V = \{0, 1\}^3, \text{ and } E = \{\{x, y\} \mid x, y \in \{0, 1\}^3 \text{ and } x, y \text{ differ in exactly 1 bit}\}.$$

18. The identity function on the vertex set of a graph is clearly an automorphism of a graph. Thus, every graph has at least one automorphism. Find the smallest graph (one having the minimum total number of vertices and edges) with at least 2 vertices which has no automorphism other than the identity.

19. Prove that the number of connected components of any graph $G = (V, E)$ is at least $|V| - |E|$.

20. Prove that a graph is a tree if and only if for any two vertices u and v, the graph contains a unique path from u to v.

21. **[Cut property of trees]** Let $G = (V, E)$ be a tree and $e \in E$ be an arbitrary edge. Prove that $G' = (V, E \setminus \{e\})$ has exactly 2 connected components. Further, prove that if u and v are vertices in different connected components of G', then the graph $G'' = (V, (E \setminus \{e\}) \cup \{\{u, v\}\})$ is also a tree.

22. Let $G = (V, E)$ be any connected graph which satisfies the above cut property, that is, for every $e \in E$, the graph $G' = (V, E \setminus \{e\})$ has exactly 2 connected components. Prove that G is a tree.

23. **[Cycle property of trees]** Let $G = (V, E)$ be a tree and u, v be vertices such that $\{u, v\} \notin E$. Prove that $G' = (V, E \cup \{\{u, v\}\})$ has exactly 1 cycle (modulo the choice of the initial vertex and the direction of traversal). Further, prove that if e is any edge in this cycle, then the graph $G'' = (V, (E \cup \{\{u, v\}\}) \setminus \{e\})$ is also a tree.

24. Let $G = (V, E)$ be any acyclic graph which satisfies the above cycle property, that is, for every two vertices u, v such that $\{u, v\} \notin E$, the graph $G' = (V, E \cup \{u, v\})$ has exactly 1 cycle (modulo the choice of the initial vertex and the direction of traversal). Prove that G is a tree.

25. A *spanning tree* of a graph G is a tree whose vertex set is the vertex set of G, and which is a subgraph of G. Prove that a graph is connected if and only if it has a spanning tree.

26. Given a number $n \in \mathbb{N}$, we wish to determine the number of trees on the vertex set $\{1, 2, \ldots, n\}$. We will do this in class for an arbitrary n, but for now, find this number for all $n \leq 6$ and come up with a conjecture for arbitrary n.

27. Recall that a graph has an Euler tour if and only if it has at most one nonempty connected component and all its vertices have an even degree. Determine a necessary and sufficient condition for a graph having at most one nonempty connected component to have an Euler walk, and prove your claim. The condition must be easily verifiable by looking at the degree sequence of the graph only.

28. A matching M in a graph $G = (V, E)$ is said to be *maximal* if the matching cannot be made larger by simply adding an edge to it, that is, there does not exist an $e \in E \setminus M$ such that $M \cup \{e\}$ is also a matching. Prove that in every graph, the size of every maximal matching is at least half the size of a maximum-size matching M^*. Also prove that this bound is tight. More generally, suppose M is a matching such that the length of every augmenting path of M is at least ℓ (where ℓ is an odd natural number). Find the minimum possible value of $|M|/|M^*|$ as a function of ℓ.

29. A *vertex cover* of a graph $G = (V, E)$ is a subset C of the vertex set such that every edge $e \in E$ has at least one of its endpoints in C. Prove that the size of the minimum-size vertex cover of every graph G is at least the size of the maximum-size matching in G. Construct an infinite set of graphs for which this bound is not tight, that is, the size of the minimum-size vertex cover of every graph G in your set is more than the size of the maximum-size matching in G.

30. **[König's Theorem]** Prove that for every bipartite graph G, the size of the minimum-size vertex cover of G **equals** the size of the maximum-size matching in G. Hint: begin your proof as follows: "Let (V_1, V_2) be a bipartition of G and let M be a maximum-size matching in G. Let S be the set of vertices that are reachable by an alternating path starting from any unmatched vertex in V_1." Is the converse true? That is, suppose G is a graph such that the size of the minimum-size vertex cover of G equals the size of the maximum-size matching in G. Is G necessarily bipartite?

31. Recall that a *directed graph* G is a pair (V, A), where V is a finite set, the set of vertices, and A, the set of *arcs* or *directed edges*, is a subset of $V \times V$. The definitions of walk, closed walk, path, and cycle in a directed graph are analogous. A walk is a sequence of vertices $v_0, v_1, \ldots, v_m$ such that $(v_{i-1}, v_i) \in A$ for each i. Such a walk is a closed walk if $v_0 = v_m$, and a path if $v_0, \ldots, v_m$ are all distinct. Such a walk is a cycle if it is a closed walk and $v_1, \ldots, v_m$ are all distinct vertices. (Observe the difference: in case of directed graphs, we could have a cycle involving only one or two vertices, which is impossible in a usual graph.) Prove that for every directed graph G, G has a closed walk if and only if G has a cycle.

32. A vertex v of a directed graph is called a *source* (resp. *sink*) if for every $u \in V$, $(u, v) \notin A$ (resp. $(v, u) \notin A$), that is, v does not have an *incoming* (resp. *outgoing*) edge. A directed graph is called a *directed acyclic graph* or a *DAG* if it does not have a directed cycle. A *topological sort* of a directed graph is an arrangement $v_1, \ldots, v_n$ of all its vertices such that there does not exist an arc of the form (v_i, v_j) for $i \geq j$ (in other words, every arc goes from an "earlier" vertex to a "later" vertex in the arrangement).

    (a) Prove that every DAG has a source and a sink.

    (b) Prove that a directed graph is a DAG if and only if it has a topological sort.

33. You are standing at the origin of the coordinate system. In every step, you either walk one step to the right or one step up. Find the number of ways you can reach the point $(m, n) \in \mathbb{N} \times \mathbb{N}$ as a function of m and n.

34. Give a combinatorial proof of the following identity. For every $m, n, k \in \mathbb{N} \cup \{0\}$, $C(m+n, k) = \sum_{i=0}^{k} C(m, i) \cdot C(n, k-i)$. (Here, $C(n, k)$ is the convenient notation we will use in our answers for "n choose k", if typesetting ${}^nC_k$ or $\binom{n}{k}$ is inconvenient.)

35. The *Euler's totient function*, denoted by ϕ, is defined as follows. For an integer n, $\phi(n)$ is the number of natural numbers in $\{1, \ldots, n\}$ that are coprime to n. Given an integer n, let $\{p_1, \ldots, p_k\}$ denote the set of all primes that divide n. Derive an expression for $\phi(n)$ in terms of n and $p_1, \ldots, p_k$.

36. Recall the definition of Catalan numbers C_n, and that we proved $C_n = C(2n, n)/(n+1)$ using generating functions. Our goal here is to derive the same expression for C_n using purely combinatorial arguments. Recall the expression for the number of ways of walking from $(0, 0)$ to (m, n) by taking unit steps to the right or up that you derived in problem 33. For convenience, let us call all such ways *canonical walks*.

    (a) Prove that the number of canonical walks from $(0, 0)$ to (n, n) that never go above the line $x = y$ (touching the line is acceptable) is equal to C_n.

    (b) Prove that the set of canonical walks from $(0, 0)$ to (n, n) that go above the line $x = y$ at least once is in bijective correspondence with the set of canonical walks from $(0, 0)$ to $(n-1, n+1)$.

    (c) Using the above two results and the expression for the number of canonical walks from problem 33, derive an expression for C_n, and prove that it is equal to $C(2n, n)/(n+1)$.

37. Solve the following recurrences using the technique of generating functions.

    (a) $a_n = 3a_{n-1} - a_{n-2}$ for $n \geq 2$, $a_0 = 0$, $a_1 = 1$.

    (b) $b_n = b_{n-1} + b_{n-2} - b_{n-3}$ for $n \geq 3$, $b_0 = 0$, $b_1 = 0$, $b_2 = 1$.

    (c) $c_n = 2c_{n-1} - c_{n-2} + 1$ for $n \geq 2$, $c_0 = 0$, $c_1 = 1$.

    (d) $d_n = d_{n-1}/n + 1/(n!)$ for $n \geq 1$, $d_0 = 1$.

38. Let $T \subseteq \mathbb{N}$ be a finite set. Let s_n^T denote the number of ways of writing n as a sum of numbers from the set T, possibly with repetition but ignoring order. For example, if $T = \{1, 2\}$, then $s_n^T = \lfloor n/2 \rfloor + 1$. Find the generating function of the sequence $s_0^T, s_1^T, \ldots$ for a given set T.

39. Prove that for every $n \in \mathbb{N}$, $n^n/e^{n-1} \leq n! \leq (n+1)^{n+1}/e^n$. Hint: Write $\ln(n!)$ as the definite integral of an appropriate function and then use JEE mathematics.

40. A *subseqence* of a sequence $a_1, \ldots, a_m$ is the sequence $a_{i_1}, a_{i_2}, \ldots, a_{i_k}$ for some $k \leq m$ and $1 \leq i_1 < i_2 < \cdots < i_k \leq m$. Prove that for every $n \in \mathbb{N}$, every sequence of more than n^2 numbers has a non-decreasing subsequence of more than n numbers or a non-increasing subsequence of more than n numbers. Prove that the claim not necessarily true for suquences of n^2 real numbers.

41. Let $n, k, \ell \in \mathbb{N}$. Consider a complete graph on n vertices in which each edge is one of ℓ colors. A subgraph of this graph is said to be *monochromatic* if all edges in the subgraph are the same color. Prove that if $n \leq (k!)^{1/k} \cdot \ell^{(k-1)/2-1/k}$, then there exists a coloring such that no clique of size k is monochromatic.

42. A *permutation* of a set S is a bijection from S to S. Let S be a finite set and G be any set of permutations of S satisfying the following properties.

    (a) The identity permutation (the one which maps every element of S to itself) is in G.

    (b) For every $f \in G$, the inverse permutation f^{-1} is also in G.

    (c) For every $f_1, f_2 \in G$, the permutation $f_1 \circ f_2$ (the composition of f_1 and f_2) is also in G.

    Define the relation R_G as $R_G = \{(x, y) \in S \times S \mid \exists f \in G \text{ such that } y = f(x)\}$. Prove that R_G is an equivalence relation.

43. Recall that given a set Σ, we defined the Σ^* to be the set of finite-length strings over the alphabet Σ. Given two strings $x, y \in \Sigma^*$, let xy denote their concatenation. For this problem, let Σ be a finite set and let $L \subseteq \Sigma^*$. Let the relation R_L on Σ^* be defined as $R_L = \{(x, y) \in \Sigma^* \times \Sigma^* \mid \forall z \in \Sigma^* \ (xz \in L \Leftrightarrow yz \in L)\}$. Prove that R_L is an equivalence relation.

44. A *finite automaton* is a (simple) computer that has the following components.

    (a) A fixed finite set Q, called the set of states.

    (b) A fixed state $q_0 \in Q$, called the initial state.

    (c) A fixed function $f : Q \times \{0, 1\} \longrightarrow Q$, called the transition function.

    (d) A fixed subset A of Q, called the set of accepting states.

    Such a finite automaton processes a binary string given as input as specified by the following algorithm.

    - $s \leftarrow q_0$. (Initialize s to the initial state.)
    - While the input is not over, do:
        - Read the next bit of input, say b.
        - $s \leftarrow f(s, b)$. (Change state as per the transition function.)
    - If $s \in A$ then output "accept", else output "reject".

    Given an $L \subseteq \{0, 1\}^*$, we would like to build a finite automaton that, on every $x \in \{0, 1\}^*$, outputs "accept" if and only if $x \in L$. Explain how you will do this if the relation R_L defined in the previous problem has only finitely many equivalence classes. (Consider some special cases for example (i) L is the set of strings containing an odd number of ones (ii) L is the set of binary representations of natural numbers divisible by 3. In each case, understand R_L, build a finite automaton, and see if you get an idea.)

45. Recall that we saw how to define the set $\mathbb{Q}$ of rational numbers starting from the set $\mathbb{Z}$ of integers using equivalence relations. Now we will define the set $\mathbb{R}$ of real numbers from $\mathbb{Q}$. Let $\mathbb{Q}_+$ denote the set of positive rational numbers. An infinite sequence $\overline{x} = (x_1, x_2, \ldots)$ of rational numbers is said to be a *Cauchy sequence* if for every $\varepsilon \in \mathbb{Q}_+$ there exists some integer N such that for all $n_1 \geq N$ and $n_2 \geq N$, $|x_{n_1} - x_{n_2}| < \varepsilon$ (that is, in plain English, the numbers in the sequence get closer and closer). Define a relation $\approx$ on the set $\mathcal{C}$ of Cauchy sequences as $\overline{x} \approx \overline{y}$ if for every $\varepsilon \in \mathbb{Q}_+$ there exists some

integer N such that for all $n \geq N$, $|x_n - y_n| < \varepsilon$. Prove that $\approx$ is an equivalence relation. Having proved this, we define $\mathbb{R} = \mathcal{C}/\approx$, that is, the set of real numbers is the set of equivalence classes of the relation $\approx$. Give at least two Cauchy sequences, containing no common element, which fall into the equivalence class of $\approx$ corresponding to the real number $\sqrt{2}$. As an extra exercise (which is out of the scope of this course) figure out how you will define the "less than" relation on two equvalence classes of $\mathcal{C}/\approx$, and how you will add and multiply two such equivalence classes.

46. Prove the following claim mentioned in class, which is known as Mirsky's theorem. Suppose (S, R) is a poset in which the largest chain has a finite size, say m (S itself could be infinite). Prove that S can be partitioned into m antichains, say $A_1, \ldots, A_m$ such that for all $x, y \in S$ such that $x \neq y$ and $(x, y) \in R$, x and y belong to some antichains, say A_i and A_j respectively, such that $i < j$. (Recall the task scheduling analogy: what set of tasks do you do in the i'th time interval, if you do every task as soon as all its pre-requisites are complete?)

47. Given a finite poset (S, R), recall that we defined the Hasse diagram of this poset via a relation H on S defined as

$$H = \{(x, y) \in S \times S \mid x \neq y,\ (x, y) \in R, \text{ and } (\nexists z \in S \text{ such that } (x, z) \in R \wedge (z, y) \in R)\}.$$

    We proved that the reflexive-transitive closure of H is R. Prove that H is the minimal relation on S whose reflexive-transitive closure is R. In other words, if H' is a relation on S whose reflexive-transitive closure is R, prove that $H \subseteq H'$.

48. Let $(G_1, *_1)$ and $(G_2, *_2)$ be groups. Define the binary operation $*$ on $G_1 \times G_2$ as $(x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1, x_2 *_2 y_2)$. Prove that $(G_1 \times G_2, *)$ is a group.

49. Let G be a group and $\mathcal{H}$ be an arbitrary collection of subgroups of G. Prove that $H^* = \bigcap_{H \in \mathcal{H}} H$ is a subgroup of G.

50. Let G be a group and S be an arbitrary subset of G. Prove that there exists a unique minimal subgroup of G (denoted by $\langle S \rangle$) which is a superset of S. That is, prove that there exists a unique subgroup $\langle S \rangle$ of G satisfying the following conditions: $\langle S \rangle \supseteq S$, and for every subgroup H of G, $S \subseteq H \Rightarrow \langle S \rangle \subseteq H$.

51. Let $(G, *)$ be a group and let x^{-1} denote the inverse of $x \in G$. Let H be a subgroup of G. Define the relations $\approx_l$ and $\approx_r$ on G as $x \approx_l y$ if $x^{-1} * y \in H$ and $x \approx_r y$ if $x * y^{-1} \in H$. Prove that $\approx_l$ and $\approx_r$ are equivalence realtions. What are the equivalence classes of these relations also known as?

52. Let $(G, *)$ be a group and let x^{-1} denote the inverse of $x \in G$. Let H be a subgroup of G, and g be an arbitrary element of G. Prove that $g * H * g^{-1} = \{g * h * g^{-1} \mid h \in H\}$ is also a subgroup of G. Define the relation $\equiv$ on the set of subgroups of G as follows. $H_1 \equiv H_2$ if there exists $g \in G$ such that $H_2 = g * H_1 * g^{-1}$. Prove that $\equiv$ is an equivalence relation. (To understand how the subgroup $g * H * g^{-1}$ is related to the subgroup H, take $G = \mathcal{S}_{\{1,\ldots,7\}}$, H to be the set of permutations of $\{1, \ldots, 7\}$ that map $\{1, 2, 3\}$ among themselves, and try a handful of permutations as g. Note down your observations.)

53. The n'th *dihedral group*, denoted by D_n, is the automorphism group of the "cycle graph" C_n on n vertices, that is, the graph whose vertex set is $V = \{0, \ldots, n-1\}$, and edge set is

$$E = \{\{0, 1\}, \{1, 2\}, \ldots, \{n-2, n-1\}, \{n-1, 0\}\}.$$

    Let σ be the permutation of V defined as $\sigma(i) = (i + 1) \bmod n$, and let π be the permutation of V defined as $\pi(0) = 0$, $\pi(i) = n - i$ for $i > 0$. Check that the automorphism group of C_n can be expressed in terms of σ and π as $\{\mathrm{id}, \sigma, \ldots, \sigma^{n-1}, \pi, \sigma\pi, \ldots, \sigma^{n-1}\pi\}$, and that $\sigma^n = \pi^2 = \mathrm{id}$, and $\pi\sigma^k = \sigma^{n-k}\pi$. Determine all the subgroups of D_n when n is a prime. For each such subgroup H, identify the left and the right cosets of H.

54. Suppose $(G, *)$ is a group and H is a subgroup of G. Prove that the following conditions are equivalent.

    (a) Every left coset of H is a right coset of H.

(b) Every right coset of H is a left coset of H.

(c) For every $g \in G$, the subgroup $g * H * g^{-1}$ is exactly the subgroup H.

If H satisfies any of (and therefore, all) the above conditions, then it is called a *normal subgroup* of G. Prove that if H is a normal subgroup of G, then the following holds. For every $x_1, x_2, y_1, y_2 \in G$, if x_1, x_2 lie in the same coset of H, and y_1, y_2 lie in the same coset of H, then $x_1 * y_1, x_2 * y_2$ also lie in the same coset of H. Thus, it is possible to define a binary operation $\bigcirc$ on the set of cosets of H (denoted by G/H) as follows: for cosets C_1, C_2 of H, $C_1 \bigcirc C_2$ is the coset of H that contains all elements of the form $x_1 * x_2$, where $x_1 \in C_1$ and $x_2 \in C_2$. Prove that $(G/H, \bigcirc)$ is a group.

55. Let φ be a homomorphism from a group G to a group H. Recall that we proved in class that every left coset of $\ker(\varphi)$ is also its right coset (and vice versa), so $\ker(\varphi)$ is a normal subgroup of G. We also proved that $\mathrm{Im}(\varphi)$, the image of the function φ, is a subgroup of H. Prove that, in fact $\mathrm{Im}(\varphi)$ is isomorphic to the group $G/\ker(\varphi)$.