CS21001 Discrete Structures

Autumn 2009–10

Solutions to Tutorial on : Groups and Graphs

---

1. Let $(S, *)$ be a semigroup and $a \in S$. The sub-semigroup generated by a is the set $\langle a \rangle = \{a * a * a \cdots a \text{ (n times)} \mid n > 0\}$. S is cyclic if $S = \langle a \rangle$ for some $a \in S$. Justify which of the following semigroups is/are cyclic.

   (a) $\mathbb{N}$ under integer multiplication.

   Solution: No. Every positive integer cannot be written as a power of a fixed (positive) integer. More precisely, suppose $\mathbb{N} = \langle a \rangle$ for some $a \in \mathbb{N}$. But then, $2 = a^i$ and $3 = a^j$ for some $i, j > 0$. But then a divides both 2 and 3, whereas $2, 3$ are coprime. Thus $a = 1$ and consequently $\langle a \rangle = \{1\} \neq \mathbb{N}$, a contradiction.

   (b) $\mathbb{Z}$ under integer addition.

   Solution: No. Consider $\langle a \rangle$ for some $a \in \mathbb{Z}$. We have $\langle a \rangle = \{0\}$. So assume $a \neq 0$. If $a > 0$, then $\langle a \rangle$ contains only positive integers. On the other hand, if $a < 0$, then $\langle a \rangle$ contains only negative integers. In all these cases, $\langle a \rangle$ is a proper subset of $\mathbb{Z}$.

   (c) $\mathbb{Z}_n$ under addition modulo n.

   Solution: Yes. $\mathbb{Z}_n$ is generated by (the equivalence class of) 1. Note that

$$\begin{aligned} 1 &\equiv 1 \text{ (mod n)}, \\ 2 &\equiv 1 + 1 \text{ (mod n)}, \\ &\cdots \\ n - 1 &\equiv 1 + 1 + \cdots + 1 \text{ (n - 1 times) (mod n), and} \\ 0 &\equiv 1 + 1 + \cdots + 1 \text{ (n times) (mod n).} \end{aligned}$$

2. Let G be a finite multiplicative group and $h = \text{ord } a$ for some $a \in G$. Show that $a^n = e$ iff $h | n$.

   Solution: [if] Let $n = kh$. Then $a^n = \left(a^h\right)^k = e^k = e$.
   [only if] Suppose $a^n = e$, where $n = qh + r$ with $0 \leq r < h$. Since $a^h = e$, it follows that $a^r = e$. Since ord a is the smallest positive integer h with property $a^h = e$, we must have $r = 0$, i.e. $n = qh$ is an integral multiple of h.

3. (a) Define an operation $*$ on $\mathbb{R}$ as $x * y = x + y + xy$. Prove or disprove: $(\mathbb{R}, *)$ is a group.

   Solution: [Closure] Obvious.
   [Associativity] We have $(x * y) * z = (x + y + xy) * z = (x + y + xy) + z + (x + y + xy)z = x + y + z + xy + yz + zx + xyz$. Similarly, $x * (y * z) = x + y + z + xy + yz + zx + xyz$. Thus, $(x * y) * z = x * (y * z)$.
   [Identity] It is easy to verify that 0 is the identity element w.r.t $*$.
   [Inverse] Let $x \in \mathbb{R}$ have the inverse $y \in \mathbb{R}$, i.e. $x * y = x + y + xy = 0$, i.e. $y = \frac{-x}{1+x}$, i.e. y exists iff $x \neq -1$. Since -1 does not have an inverse under $*$, $(\mathbb{R}, *)$ is not a group.

   (b) Prove or disprove: $(\mathbb{R} \setminus \{-1\}, *)$ is a group.

   Solution: The closure is the only property that requires to be verified. Take $x, y \in \mathbb{R}$. Then, $(1+x)(1+y) \neq 0$, i.e. $x + y + xy \neq -1$, i.e. $\mathbb{R} \setminus \{-1\}$ is closed under $*$.

4. Let G be an Abelian group. An element $a \in G$ is called a *torsion element* of G if ord a is finite. Prove that the set of all torsion elements of G is a subgroup of G.

Solution: We denote by H the set of all elements of G of finite orders.
[Closure] Let $a, b \in H$, ord $a = m$ and ord $b = n$. But then, $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e$, i.e. ord$(ab)|mn$. In particular, ord$(ab)$ is finite, i.e. $ab \in H$.
[Inverse] Let $a \in H$. Since $a^k = e$ iff $(a^k)^{-1} = (a^{-1})^k = e$, we have ord$(a^{-1})$ = ord a.

5. Let G be a multiplicative group and H, K subgroups of G with $H \cap K = \{e\}$. Assume that $G = HK = \{hk|h \in H, k \in K\}$. Prove that every element $a \in G$ can be written as $a = hk$ for some unique elements $h \in H$ and $k \in K$.

   Solution: Let $a \in G$ be written as $a = h_1k_1 = h_2k_2$ with $h_1, h_2 \in H$ and $k_1, k_2 \in K$. The element $h_1^{-1}h_2 = k_1k_2^{-1}$ belongs to $H \cap K$ and is the identity element by hypothesis. But then $h_1 = h_2$ and $k_1 = k_2$.

6. Show that the set of all complex numbers of the form $x + \mathrm{i}y$ with x, y integers and with x even is a group under addition of complex numbers.

   Solution: It suffices only to check closure and inverse. If x,y,x',y' are integers then $x + x'$ and $y + y'$ are also integers. Moreover, if x and x' are even, then so also is $x + x'$. Finally, the inverse of $x + \mathrm{i}y$ is $-x - \mathrm{i}y$. Here $-x$, $-y$ are also integers and $-x$ is also even (if x is so).

7. Prove that an undirected graph has an even number of vertices of odd degree.

   Solution: Let V_1 and V_2 be the set of vertices of even degree and odd degree, respectively, in an undirected graph $G = (V, E)$. Then

$$2e = \sum_{\in V} \text{deg}() = \sum_{\in V_1} \text{deg}() + \sum_{\in V_2} \text{deg}()$$

   Since deg() is even for $\in V_1$, the first term in the R.H.S of the last equality is even. Furthermore, the sum of the two terms on the R.H.S of the last equality is even, because this sum is $2e$. Hence, the second term in the sum is also even. Because, all the terms in this sum are odd, there must be an even number of such terms. Thus, there are an even number of vertices of odd degree.

8. Show that a graph is bipartite iff it has no odd cycles.

   Solution: [if] It is possible to color the graph with 2 colors. If the graph contained an odd cycle, that would not have been possible.
   [only if] Assume the graph has no odd cycles and consider a spanning tree of the graph. Start from a vertex of this tree (call this *root*) and color this vertex red. Now color the graph with green, for adjacent vertices. The distance of the red vertices from the root is even while green vertices are at odd distances. Consider an edge e of the graph that connects vertex x to y. It is sufficient to show that (each) edge e cannot connect two red or two green vertices. If e belongs to this spanning tree then this is true from construction. Now, if e does not belong to this tree, then there exists a cycle in the graph which contains e. However, this cycle is even by the initial assumption. Thus the vertices x and y cannot have the same color, which proves the graph to be bipartite.

9. Let $G = (V, E)$ be a graph with $|V| = n$. Let the maximum degree of any node be at most d and a vertex cover of G be of size at most c. Find the maximum number of edges that G can have.

   Solution: Let $V' \subseteq V$ be a vertex cover in G of size $c' \leq c$. As V' is a vertex cover, every edge in G has at least one of its vertices in V'. Also, each node having a degree of at most d can cover at most d edges. Thus we can have a total of $c'd \leq cd$ edges in G.

10. If α and β denote the minimum vertex cover and maximum independent set respectively of an undirected connected graph G with n vertices, then $\alpha + \beta = n$. Prove or disprove the above statement.

    Solution: For any two vertices in the maximum independent set of size β, there is no edge joining the two vertices. So, the remaining $n - \beta$ vertices will definitely form a vertex cover (not necessarily minimum). Thus, $\alpha \leq n - \beta$. On the other hand, for any two vertices not in the minimum vertex cover of size α, there can be no edge between two such vertices. So, these vertices form an independent set of size $n - \alpha$ (not necessarily maximum). Thus, $\beta \geq n - \alpha$. From the two inequalities, we have $\alpha + \beta \leq n$ and $\alpha + \beta \geq n$, which proves the above statement.