Tutorial 8 Solutions

1a) $(a * b) * c = (a + b - ab) * c$

$= (a+b-ab) + c - (a+b-ab) * c \rightarrow a+b+c - ab - ac - bc - abc$

similarly we can show for $a * (b * c)$

Thus * is associative (Q,*) is a semigroup

$a * b = a + b - ab = b + a - ab = b * a$

Hence (Q,*) is commutative

b) $a * e = a \ (where\ e\ is\ an\ identity\ element)$

$a + e - ae = a \Rightarrow e - ae = 0 \Rightarrow e(1-a) = 0 \Rightarrow e = 0$

c) 0 in identity element

a * x = 0 (x in inverse)

$a + x - ax = 0 \rightarrow x = \frac{a}{a-1}$

$a \neq 1 inverse\ of\ a\ is\ x$

2) $b * (a * b') = b * e = b \ and\ (b * a) * b' = e * b' = b'$

$Since\ S\ is\ associative\ b * (a * b') = (b * a) * b'\ hence\ b = b'$

3) a) Use associative property to show semigroup

b) $f(x * y) = f(a + c, b + b) = (a + c) - (b + d) = (a - b) + (c - d) = f(x)f(y) \rightarrow f\ is\ a\ homomorphism$

c) Suppose f(x) = f(y) $\rightarrow a - b = c - d \Rightarrow a + d = b + c \quad Thus\ (a,b) \sim (c,d)\ if\ a + d = b + c$

4)

Solution Let G be an infinite multiplicative group. If G has an element a of infinite order, then for every $n \in \mathbb{N}$, G has a subgroup generated by g^n. These subgroups are different for different values of n.

Finally assume that all elements of G have finite orders. Let $a_1, a_2, \ldots, a_n, \ldots$ be distinct elements of G. Consider the subgroups $H_n = \langle a_n \rangle$ for all $n \in \mathbb{N}$. Suppose that there are only finitely many different subgroups in the family $H_1, H_2, H_3, \ldots$ of subgroups. This means there exists an $n \in \mathbb{N}$ such that $H_n = H_{n+1} = H_{n+2} = \cdots$. But a_n is of finite order, i.e., H_n is a finite group and cannot contain all of the infinitely many elements $a_{n+1}, a_{n+2}, a_{n+3}, \ldots$. If $a_m \notin H_n$ for some $m > n$, then $H_m \neq H_n$, a contradiction.

5)

Since G is cyclic, there is an element a in G such that $G = gp(a)$. Let H be a subgroup of G. If $H = \{e\}$, then $H = gp(e)$ and is cyclic. Otherwise, H contains a nonzero power of a. Since H is a subgroup, it must be closed under inverses and so contains positive powers of a. Let m be the smallest positive power of a such that a^m belongs to H. We claim that $b = a^m$ generates H. Let x be any other element of H; since x belongs to G we have $x = a^n$ for some integer n. Dividing n by m we get a quotient q and a remainder r, i.e.,

$$n = mq + r$$

where $0 \leq r < m$. Then

$$a^n = a^{mq+r} = a^{mq} \cdot a^r = b^q \cdot a^r \qquad \text{so} \qquad a^r = b^{-q}a^n$$

But a^n, $b \in H$. Since H is a subgroup, $b^{-q}a^n \in H$, which means $a^r \in H$. However, m was the smallest positive power of a belonging to H. Therefore $r = 0$. Hence $a^n = b^q$. Thus b generates H, and so H is cyclic.

6)

(*a*) Since $e = ee$ and f is a homomorphism, we have

$$f(e) = f(ee) = f(e)f(e)$$

Multiplying both sides by $f(e)^{-1}$ gives us our result.

(*b*) Using part (*a*) and that $aa^{-1} = a^{-1}a = e$, we have

$$e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1}) \qquad \text{and} \qquad e' = f(e) = f(a^{-1}a) = f(a^{-1})f(a)$$

Hence $f(a^{-1})$ is the inverse of $f(a)$; that is, $f(a^{-1}) = f(a)^{-1}$.

7) Suppose m is the order of g(a) . Then $a^m = e$ Also by lagrange's theorem m divides n , say n = mr Then

$$a^n = a^{mr} = (a^m)^r = e^r = e$$

[Lagrange Theorem : let H be a subgroup of a finite group G Then the order of H divides the order of G.

One can actually show that the number of right cosets of H in G , called the index of H in g , is equal to the number of left cosets of H in G; and both number are equal to |G| divided by |H|]