M311S24 Problem Set 2 *Franchi-Pereira, Philip*

Problem 1.a Let S be a semigroup with some (not necessarily unique) left neutral element e_L, and such that any element a has a left inverse b_L with respect to e_L. Show that S is in fact a group.

Lemma 1 All left inverses b_L with respect to e_L in S are also right inverses.

Proof Note that since $b_L \in S$, then it too has an inverse, denoted by b_L^{-1}, such that $b_L^{-1} b_L = e_L$. Then by associativity and the definition of our inverses:

$$\begin{aligned} b_L a = e_L = b_L^{-1} b_L = b_L^{-1}(e\, b_L) = b_L^{-1}((b_L a) b_L) \\ = (b_L^{-1} b_L)(a b_L) = e(a b_L) = a b_L \end{aligned}$$

Lemma 2 If $e_L$is a left neutral of S, then it is also a right neutral.

Proof Since $e_L \in S$, it has a left inverse: $e_L e_L = e_L$. By Lemma 1, it must also have a right inverse, e_R, such that $e_L e_R = e_L$. But then we see that $e_R = e_L e_R = e_L$, and so the neutral element e is unique.

Lemma 3 The every element $a \in S$ has a left inverse b_L and right inverse b_R, then $b_L = b_R = b$.

Proof Note that $b_L = b_L e = b_L(a b_r)$, and by associativity, $b_L(a b_r) = (b_L a) b_R = e b_R = b_R$. Therefore $b_L = b_R$.

Lemma 4 The inverse of any element $a \in S$ is unique, denoted by a^{-1}.

Proof Let b_0, b_1 be inverses of a. Then by similar logic to the previous lemma,

$$b_1 = b_1 e = b_1(a b_0) \text{ and by associativity } b_1(a b_0) = (b_1 a) b_0 = e b_0 = b_0$$

Since the semigroup S contains a unique identity element, every element in S has a unique inverse, and the operation over S, Δ is associative, then by definition S is actually a group

1.b Let S be a semigroup which has a left neutral e_L and such that any element a has a right inverse b_R with respect to e_L. Is S necessarily a group? Prove or give a counter-example.

Counter Example: Let $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \phi(a, b) \mapsto b$. We will show that ϕ is associative

$$(ab)c = (b)c = (bc) = c$$

$$a(bc) = a(c) = (ac) = c$$

So $\mathbb{Z}, \phi$ is a semigroup. Furthermore, every integer can be a left neutral element, since for any $b \in \mathbb{Z}$, all elements $a \in \mathbb{Z}$ by definition give $\phi(a, b) =$

b. Finally, every element $a \in \mathbb{Z}$ has a right inverses with respect to e_L. Since e_L can be any integer, any $a, b \in \mathbb{Z}$ produces e_L.

However, ϕ is not a group. The only choice of right neutral element such that $ae = a,\ a, e \in \mathbb{Z}$ is a itself, but any integer can be left neutral. Therefore there is no unique neutral element, and so ϕ is not a group.

Problem 2.a Let G be a group such that for all $g \in G,\ g^2 = e$. Prove that G is abelian.

Proof: Let $a, b \in G$. To show that $ab = ba$, note that the inverse of ab is ba, since $(ba)(ab) = b(aa)b = bb = e$. Note also that $(ba)^2 = e$ by definition. It follows that $ab = e(ab) = ((ba)(ba))(ab) = (ba)((ba)(ab)) = (ba)e = ba$.

2.b Suppose, instead we have for all $g \in G,\ g^3 = e$. Is G necessarily abelian? Prove or give a counterexample.

Problem 3 Let G be finite group and let $2|o(G)$. Prove that G has an odd number of elements of order 2. In particular G has at least one element of order 2.

Problem 4 Let H and K be subgroups of a group. Prove that $H \cap K$ is a subgroup of G.

Proof: For all $a, b \in H \cap K,\ a, b \in H$. Since H is also a group, then clearly $ab^{-1} \in H$. Likewise, $a, b \in K$, so $ab^{-1} \in K$. Since ab^{-1} is in both H and K, $ab^{-1} \in H \cap K$. Therefore by BB.Corollary 3.2.3, $H \cap K$ is a subgroup of G.

Problem 5 Fill out the table. The first row of the table was computed using Python.

(m,n)	md(m,n)	qt(m,n)
(987654321, 7531)	1326	131145
(987654321, -7531)	1326	-131145
(-987654321, 7531)	-1326	-131146
(-987654321, -7531)	6205	131146

Problem 6 Let a and b be positive integers. Let $a = h(a, b),\ b = k(a, b)$. Take any pair ω, γ with $\omega a + \gamma b = (a, b)$. Show that $(\omega, \gamma) = 1$ and $(h, k) = 1$.

Proof: Let $d = (a, b)$, the GCD of a and b. Then $a = kd,\ b = kd$ and $\omega a + \gamma b = d$. It follows that $\omega a + \gamma b = \omega(hd) + \gamma(kd) = (\omega h + \gamma k)d = d$. Then by BB A3.6.n, $(\omega h + \gamma k) = 1$ and so by definition, $(\omega, \gamma) = 1$ and $(h, k) = 1$.

Problem 7 Let a, b, a_1, b_1 be non-zero integers. Assume that $(a, b) = 1$ and $(a_1, b_1) = 1$ and that $ab_1 = a_1 b$ show that either $a = a_1,\ b = b_1$ or $a = -a_1,\ b = -b_1$.

Problem 8 Find (a, b) and ω and γ such that $(\omega, \gamma) = (a, b)$ for (1) $a = 26460, b = 126000$ and (2) $a = 12091, b = 8439$

Note: The role of qt was performed by $a//b$ in Python, and md by $a\%b$ in Python.

1. $a = 26460, b = 126000$. As provided, this is 0. Assuming instead that a is the larger value of the two, then instead we have:

$$\begin{aligned} 126000 &= 26460(4) + 20160 \\ 26460 &= 20160(1) + 6300 \\ 20160 &= 6300(3) + 1260 \\ 6300 &= 1260(5) + 0 \end{aligned}$$

   So $\gcd(126000, 26460) = 1260$.

2. $a = 12091, b = 8439$

$$\begin{aligned} 12091 &= 8439(1) + 3652 \\ 8439 &= 3652(2) + 1135 \\ 3652 &= 1135(3) + 247 \\ 1135 &= 247(4) + 147 \\ 247 &= 147(1) + 100 \\ 147 &= 100(1) + 47 \\ 100 &= 47(2) + 6 \\ 47 &= 6(7) + 5 \\ 6 &= 5(1) + 1 \\ 5 &= 1(5) + 0 \end{aligned}$$

   Therefore these two numbers are relatively prime.

Problem 9.a The set $a\mathbb{Z} \cap b\mathbb{Z}$ is by definition the set of common multiples of a and b. Cite a result that shows that $a\mathbb{Z} \cap b\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. Why is this subgroup non-trivial?

In Problem 4 we proved that the intersection of two subgroups is itself a subgroup. It is nontrivial since $0, ab, -ab \in a\mathbb{Z}$ and $0, ab, -ab \in b\mathbb{Z}$, so it is clearly not empty.

9.b Use our results on subgroups of $\mathbb{Z}$ to show that the smallest positive common multiple of a and $b$is in fact the least common multiple.

Proof: Let $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, the set of all multiples of both a and b. This set is clearly not empty, since both $a\mathbb{Z}$ and $b\mathbb{Z}$ contain ab. Take $m\mathbb{Z} \cap \mathbb{N}$, denoted $m\mathbb{Z}^+$. Clearly every element in it is positive, and so by the Well Ordering Principle, this set has a smallest element, l, such that for all $x \in m\mathbb{Z}^+$, $l \leq x$. However, since every element in $m\mathbb{Z}^+$ is a common multiple of both a and b, then l must be the smallest positive common multiple of a, b

9.c Take $a = h(a, b)$ and $b = k(a, b)$. Which previous result shows that h and k are relatively prime?

This was shown directly in Problem 6.

9.d Let c be a common multiple of a and b. Certainly $(a,b)|c$ so we have $c = n(a,b)$. Show that $k|n$ and $h|n$. What result allows us to conclude that $hk|n$?

Proof: Since c is a multiple of a and $a = h(a,b)$, then there must exist some m_1 such that $c = m_1 h(a,b)$. Likewise c is a multiple of b and so there must be an m_2 such that $c = m_2 k(a,b)$. By the result of Problem 6, h and k are relatively prime, and so $c = m_3 hk(a,b)$** for some m_3. Therefore $hk|n$

9.e Show that $[a,b] = hk(a,b)$.

Proof: First note that $ab = (h(a,b))(k(a,b)) = hk(a,b)(a,b)$.

Problem 10 The positive numbers a and b are such that $a + b = 57$ and $[a,b] = 680$. What are a and b?

$a = 17$ and $b = 40$. First, find all the prime factors of 680. This is made easier by the fact that it is even, and so $680/2/2/2 = 85$. Then, factoring out 5, $85/5 = 17$, so $680 = 2 * 2 * 2 * 5 * 17$. Since $a + b = 57$, $a = 17$ and $b = 40$. Since a and b do not share factors, $(a,b) = 1$ and $[a,b] = \frac{|ab|}{(a,b)} = \frac{|ab|}{1} = 680$.

Problem 11

Problem 12 We are given that $n(n+30)$ a perfect square. What are the possible values of n?