EXAM 2: SOLUTIONS - MATH 341
INSTRUCTOR: George Voutsadakis

Problem 1 *Let G be a nonempty finite set closed under an associative operation such that both the left and the right cancellation laws hold. Show that G under this operation is a group.*

Solution:
Suppose that G is a nonempty finite set closed under an operation $*$, such that

1. $*$ is associative, i.e., $(a*b)*c = a*(b*c)$, for all $a,b,c \in G$,
2. the left cancellation law for $*$ holds, i.e., $a*b = a*c$ implies $b = c$, for all $a,b,c \in G$, and
3. the right cancellation law for $*$ holds, i.e., $b*a = c*a$ implies $b = c$, for all $a,b,c \in G$.

To show that under these conditions $\langle G, * \rangle$ is a group we need to prove that it has an identity and that every element in G has an inverse in G with respect to $*$.

Let $a \in G$, which exists since $G \neq \emptyset$. Consider the set

$$A = \{a^n := \underbrace{a*a*\ldots*a}_{n} : n \geq 1\} \subseteq G.$$

Since G is finite, there exist $n, m \in \mathbf{N}^*$, with $m < n$, such that $a^m = a^n$. Hence $a^m = a^{m+(n-m)}$, whence $a^m = a^m * a^{n-m}$. Now set $e := a^{n-m}$. we will show that this e is the identity in G for $*$, i.e., that $b*e = e*b = b$, for all $b \in G$. We have

$$\begin{aligned} b*a^m &= (b*a^m)*a^{n-m} \\ &= b*(a^m*a^{n-m}) \\ &= b*(a^{n-m}*a^m) \\ &= (b*a^{n-m})*a^m \\ &= (b*e)*a^m. \end{aligned}$$

Now the right cancellation law applies to give $b = b*e$. For the left-hand side identity we work symmetrically.

Now consider $b \in G$. We have, as above for a that $b^p = b^q$, for some $p, q \in \mathbf{N}^*$, with $p < q$. Then $b^p * e = b^q = b^p * b^{q-p}$, whence, by the left cancellation law, $e = b^{q-p}$. Since $q - p \geq 1$, we either have $q - p = 1$ or $q - p > 1$. If $q - p = 1$, then $b = e$, whence $e^{-1} = e$. If $q - p > 1$, then $e = b * b^{q-p-1} = b^{q-p-1} * b$, whence $b^{-1} = b^{q-p-1}$. Thus, in every case b has an inverse in G with respect to $*$. This shows that $\langle G, * \rangle$ is a group. ■

Problem 2 *Let G be a group, $a \in G$ and m, n relatively prime integers. Show that if $a^m = e$, then there exists an element $b \in G$, such that $a = b^n$.*

Solution:

Since $a^m = e$ we must have that $|a| \backslash m$, i.e., there exists a positive integer k, such that $m = k|a|$. Now m, n relatively prime implies that there exist integers x, y, such that $xm + yn = 1$. Combining the two previous relations, we obtain $xk|a| + yn = 1$.

Now set $b = a^y \in G$. We have

$$\begin{aligned} b^n &= (a^y)^n \\ &= a^{yn} \\ &= a^{1-xk|a|} \\ &= a(a^{|a|})^{-xk} \\ &= a. \end{aligned}$$

■

Problem 3 *Let G be a group and $a \in G$. Show that the centralizer $C(a)$ is a subgroup of G.*

Solution:

Suppose that $b, c \in C(a)$, i.e., $ab = ba$ and $ac = ca$. We first show that $bc \in C(a)$, i.e., that $a(bc) = (bc)a$. We have

$$\begin{aligned} a(bc) &= (ab)c \\ &= (ba)c \\ &= b(ac) \\ &= b(ca) \\ &= (bc)a. \end{aligned}$$

Finally, we show that $b^{-1} \in C(a)$, i.e., $ab^{-1} = b^{-1}a$. Since $b \in C(a)$, we get $ab = ba$, whence $b^{-1}abb^{-1} = b^{-1}bab^{-1}$ and, therefore, $b^{-1}a = ab^{-1}$. ■

Problem 4 *The* **stochastic group** $\Sigma(2, \mathbb{R})$ *consists of all those matrices in* $\mathrm{GL}(2, \mathbb{R})$ *whose column sums are 1. Show that this is in fact a subgroup of* $\mathrm{GL}(2, \mathbb{R})$.

Solution:

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} x & y \\ z & w \end{bmatrix} \in \Sigma(2, \mathbb{R})$. We thus have $a + c = b + d = 1$ and $x + z = y + w = 1$. We show that $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} \in \Sigma(2, \mathbb{R})$. We have $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} ax + bz & ay + bw \\ cx + dz & cy + dw \end{bmatrix} \in \Sigma(2, \mathbb{R})$, since $ax + bz + cx + dz = (a + c)x + (b + d)z = x + z = 1$ and $ay + bw + cy + dw = (a + c)y + (b + d)w = y + w = 1$.

To show that $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} \in \Sigma(2, \mathbb{R})$, note that

$$ad - bc = a(1 - b) - b(1 - a) = a - ab - b + ab = a - b$$

and, similarly

$$ad - bc = (1 - c)d - (1 - d)c = d - cd - c + dc = d - c.$$

Therefore $\frac{d}{ad-bc} + \frac{-c}{ad-bc} = \frac{d-c}{ad-bc} = 1$ and $\frac{-b}{ad-bc} + \frac{a}{ad-bc} = \frac{a-b}{ad-bc} = 1$. ■

Problem 5 *1. Let $G = \langle a \rangle$ be a cyclic subgroup of order 20. Find all the elements $b \in G$ of order $|b| = 10$.*

2. Let H and K be cyclic subgroups of an Abelian group G, with $|H| = 10$ and $|K| = 14$. Show that G contains a cyclic subgroup of order 70.

Solution:

1. Let $b = a^n$ be such that $|b| = 10$. Then $|a^n| = 10$, whence $\frac{20}{\gcd(n,20)} = 10$. Therefore, we must have $\gcd(n, 20) = 2$. The only four numbers $1 \leq n \leq 20$ that satisfy this condition are $2, 6, 14$ and 18. Hence

$$a^2, a^6, a^{14}, a^{18}$$

is the list of all elements in G of order 10.

2. Let $H = \langle a \rangle$ and $K = \langle b \rangle$, with $|a| = 10$ and $|b| = 14$. Then the element $a^2 \in H$ has order $|a^2| = 5$. We claim that $|a^2 b| = 70$, whence the element $a^2 b \in G$ generates a cyclic subgroup of order 70.

First note that $(a^2 b)^{70} = (a^2)^{70} b^{70} = a^{140} b^{70} = (a^{10})^{14} (b^{14})^5 = e$.

Suppose that $(a^2 b)^n = e$. Then $a^{2n} b^n = e$, whence $a^{2n} = b^{-n} \in \langle a^2 \rangle \cap K$. But $\langle a^2 \rangle \cap K = \{e\}$, since their orders are relatively prime, whence we must have $a^{2n} = e = b^n$. Therefore $5 \backslash n$ and $14 \backslash n$, whence $70 \backslash n$, i.e., $n \geq 70$. This proves that $|a^2 b| = 70$, as was to be shown.

■