Algebraic Structures: Solutions to Homework 1:

written by Motke Porat

November 2017

Question 4:

(a) Let G be a group and assume there are two unit elements in G, say $e_1 \in G$ and $e_2 \in G$. From the assumption we know that

$$e_1 g = g e_1 = g \quad \text{and} \quad e_2 h = h e_2 = h, \qquad \text{for every } g, h \in G.$$

Choosing $g = e_2$ and $h = e_1$ lead us to the conclusion that

$$e_2 = g = e_1 g = e_1 e_2 = h e_2 = h = e_1,$$

which means $e_1 = e_2$ and there is a unique unit element in G.

(b) Assume (G, e) is a group and there exists an element $h \in G$ such that $hg = g$ for all elements $g \in G$. If we choose $g = e$, then $he = e$. On the other hand, as e is the unit element of G, we know that $he = h$ and therefore $h = e$.

Question 5: To prove that a subset H of a group G is a subgroup of G we only need to show that $H \neq \emptyset$ and the property that

$$a, b \in H \Longrightarrow b^{-1} a \in H.$$

i. This H **is not a subgroup**: It is not a subset of GL_n. The matrix $0_{n\times n}$ is an upper triangular matrix but is not in invertible.

ii. $H = \{A \in GL_n(Q) : A \text{ is upper triangular}\}$ **is a subgroup**:

- $I_n \in H$ so $H \neq \emptyset$;
- If $A, B \in H$ then B is invertible and its inverse matrix B^{-1} is also upper triangular which implies that $B^{-1}A$ is invertible and upper triangular, as a product of two invertible, upper triangular matrices, i.e., $B^{-1}A \in H$.

iii. $H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, c \in \{-1, 1\}, b \in \mathbb{R} \right\}$ **is a subgroup**:

- $I_2 \in H$, so $H \neq \emptyset$.
- If $A = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \in H$ and $B = \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} \in H$, then $a_1, a_2, c_1, c_2 \in \{-1, 1\}$ and

  $$B^{-1}A = \begin{pmatrix} a_2^{-1} & -a_2^{-1} b_2 c_2^{-1} \\ 0 & c_2^{-1} \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} = \begin{pmatrix} a_2^{-1} a_1 & a_2^{-1} b_1 - a_2^{-1} b_2 c_2^{-1} c_1 \\ 0 & c_2^{-1} c_1 \end{pmatrix} \in H,$$

  since $a_2^{-1} a_1, c_2^{-1} c_1 \in \{-1, 1\}$

iv This H **is not a subgroup**: It is not closed under the (operation) product- $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in H$ but $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = I_2 \notin H$.

v. $O(3)$ **is a subgroup**:

- $I_3 \in O(3)$ and so $H \neq \emptyset$;
- If $A, B \in O(3)$, then $AA^t = BB^t = I_3$ and hence both A and B are invertible matrices and therefore we also have $B^tB = I_3$. Next,

  $$(B^{-1}A)(B^{-1}A)^t = B^{-1}AA^t(B^{-1})^t = B^{-1}(B^{-1})^t = (B^tB)^{-1} = I_3^{-1} = I_3$$

  which proves that $B^{-1}A \in O(3)$.

vi. This H **is not a subgroup**: It is not closed under the product. Let $n = 2$, so $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in H$ but $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^2 = I_2 \notin H$.

vii. This $H = Mat_{n\times n}^{sym}(\mathbb{C}) \cap GL_n(\mathbb{C})$ **is not a subgroup**: It is not closed under the product. Let $n = 2$, so $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in H$ but

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \notin H.$$

viii. This H **is not a subgroup**: It is not closed under the product. Let $n = 2, A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$. Both A and B are invertible and diagonalizable (the simplest way to see this is that both A and B are 2×2 matrices and they have 2 different eigenvalues), but

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

is not diagonalizable! (otherwise AB must be similar to the diagonal matrix with its eigenvalues on the diagonal which is equal to I_2, and the only matrix that is similar to I_2 is I_2 itself, and clearly $AB \neq I_2$) and hence $AB \notin H$.

Question 6:

(a) We will show that $(\mathbb{Z}_n, +, 0)$ **is an abelian group.** Recall the notation $\mathbb{Z}_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$ and that $\overline{n} + \overline{m} = \overline{n+m}$.

- If $\overline{a}, \overline{b} \in \mathbb{Z}_n$, then $\overline{a} + \overline{b} = \overline{a+b} \in \mathbb{Z}_n$.
- If $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$, then

  $$(\overline{a} + \overline{b}) + \overline{c} = \overline{a+b} + \overline{c} = \overline{a+b+c} = \overline{a} + \overline{b+c} = \overline{a} + (\overline{b} + \overline{c}).$$

- If $\overline{a} \in \mathbb{Z}_n$, then $\overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a}$ and $\overline{0} \in \mathbb{Z}_n$.
- If $\overline{a} \in \mathbb{Z}_n$, then $\overline{a} + \overline{-a} = \overline{-a} + \overline{a} = 0$ and $\overline{-a} \in \mathbb{Z}_n$.

This 4 properties prove that this is a group; It is an abelian group simply because of the following-

$$\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}.$$

(b) $(\mathbb{Z}_n \setminus \{\overline{0}\}, \cdot, \overline{1})$ **is a group if and only if** n **is a prime number.** This is easy to show that the first 3 properties in the definition of a group hold and that the tricky one is the forth one. We show that the fourth one holds if n is prime and it doesn't hold if n is not prime:

- If n is a prime number, then for every $\overline{a} \in \mathbb{Z}_n \setminus \{\overline{0}\}$ we know (from the Lemma of Eucleades) that the numbers a and n are coprime and therefore there exist $u, v \in \mathbb{Z}$ such that $ua + vn = 1$. Then we see that $\overline{1} = \overline{ua + vn} = \overline{ua} + \overline{0} = \overline{u} \cdot \overline{a}$ which implies that $\overline{a}$ is invertible and in fact its inverse is given by $(\overline{a})^{-1} = \overline{u}$.
- If n is not a prime, then there exist $n_1, n_2 \in \mathbb{Z}$ such that $n = n_1 n_2$ and $1 < n_1, n_2 < n$. In this case we get that

$$\overline{n_1} \cdot \overline{n_2} = \overline{n} = \overline{0}$$

  and so $\overline{n_1}$ and $\overline{n_2}$ are not invertible in $\mathbb{Z}_n \setminus \{\overline{0}\}$ and it is not a group.

Question 9:

(a)
- Consider the element $\overline{1} \in \mathbb{Z}_n$: $\overline{1} + \overline{1} = \overline{2}, \overline{1} + \overline{1} + \overline{1} = \overline{3}, ...$ and we see that if we add $\overline{1}$ m many times we get $\overline{m}$, therefore the group $\mathbb{Z}_n$ is generated by the element $\overline{1}$ and the group is cyclic.
- All the generators of the group $(\mathbb{Z}_{12}, 0, +)$ are the elements $\overline{a}$ such that a and n are coprime, and these are: $\overline{1}, \overline{5}, \overline{7}$ and $\overline{11}$.

(b)
- The group $(\mathbb{Z}_7 \setminus \{\overline{0}\}, \cdot, 1)$ is generated by the element $\overline{3}$, as

$$\overline{3} = \overline{3}, \overline{3}^2 = \overline{2}, \overline{3}^3 = 6, \overline{3}^4 = 4, \overline{3}^5 = 5 \quad \text{and} \quad \overline{3}^6 = 1$$

  and hence $\mathbb{Z}_7 \setminus \{\overline{0}\} = \{\overline{3}, \overline{3}^2, \overline{3}^3, \overline{3}^4, \overline{3}^5, \overline{3}^6\}$ is cyclic.
- The only generators of $\mathbb{Z}_7 \setminus \{\overline{0}\}$ are $\overline{3}$ and $\overline{5}$.
- The group $(\mathbb{Z}_{11} \setminus \{\overline{0}\}, \cdot, 1)$ is also cyclic and all of its generators are $\overline{2}, \overline{6}, \overline{6}$ and $\overline{8}$.

Question 10: Let $(G, \cdot, e)$ be a group of finite order, say $|G| = k$.

(a) For every $a \in G$, consider the set of powers $A = \{a, a^2, ..., a^k\} \subseteq G$.

- If $a^i = a^j$ for some $1 \leq i < j \leq k$, then $a^{j-i} = e$ and $j - i > 0$, so $n = j - i$ satisfies $a^n = e$ and $n > 0$.
- Otherwise, $a^i \neq a^j$ for all $1 \leq i, j \leq k$. But then we have k different elements in A, which means that one of them must be equal to e. So there exist $1 \leq i \leq k$ such that $a^i = e$, and we are done.

(b) From part **(a)** we know that for every $a \in G$ there exists $n_a > 0$ such that $a^{n_a} = e$. Define m to be the product of all n_a for all $a \in G$, i.e., let

$$m := \prod_{a \in G} n_a.$$

Then $m > 0$ and for every $b \in G$, we have

$$b^m = b^{n_b \prod_{a \in G, a \neq b} n_a} = (b^{n_b})^{\prod_{a \in G, a \neq b} n_a} = e^{\prod_{a \in G, a \neq b} n_a} = e.$$

(c) Let us write explicitly the elements of the group $G = \{e, g_1, ..., g_{k-1}\}$, where we know that k is even.

If for every $e \neq a \in G$ we assume that $a^{-1} \neq a$, Consider the set

$$A = \{(a, a^{-1}) : a \in G\} = \{(e, e), (g_1, g_1^{-1}), ..., (g_{k-1}, g_{k-1}^{-1})\}.$$

By our assumption, $g_1^{-1} \neq g_1, ..., g_{k-1}^{-1} \neq g_{k-1}$ and so we can throw away some of the pairs $(g_1, g_1^{-1}), ..., (g_{k-1}, g_{k-1}^{-1})$ which correspond to the same pair of elements, until we stay only with pairs which consist all of different elements and (e, e). This new list should give us all the elements in G. But then we get that in G there is an odd number of elements, which is a contradiction and therefore there exist $a \in G$ auch that $a \neq e$ and $a^{-1} = a$.