Solutions: Homework 2

January 28, 2020

Problem 1. Is $7\mathbb{Z}$ a subgroup of $(\mathbb{C}, +)$? If yes, prove it. If not, explain why not.

Proof. We first check whether $7\mathbb{Z}$ is closed under $+$. Let $a, b \in 7\mathbb{Z}$. Then $a = 7m, b = 7n$ for some $m, n \in \mathbb{Z}$. Then $a + b = 7(m + n) \in 7\mathbb{Z}$. So $7\mathbb{Z}$ is closed under $+$. 0 is the identity in $(\mathbb{C}, +)$ and obviously, $0 \in 7\mathbb{Z}$. Let $a \in 7\mathbb{Z}$. Then $a = 7n$ for some $n \in \mathbb{Z}$. Clearly, $7(-n) \in 7\mathbb{Z}$, so the inverse of a is also in $7\mathbb{Z}$. Hence, $7\mathbb{Z}$ is a subgroup of $(\mathbb{C}, +)$. □

Problem 2. Is the set $\{\pi^n | n \in \mathbb{Z}\}$ a subgroup $(\mathbb{C}, +)$? If yes, prove it. If not, explain why not.

Proof. It is not a subgroup as it is not closed under $+$, because $1 \in \{\pi^n | n \in \mathbb{Z}\}$ but $2 = 1+1$ is not in $\{\pi^n | n \in \mathbb{Z}\}$. □

Problem 3. Is the set $S = \{A \in GL_n(\mathbb{R}) | \det(A) = \pm 1\}$ a subgroup of $(GL_n(\mathbb{R}), .)$? If yes, prove it. If not, explain why not.

Proof. Let $A, B \in S$. Then, $\det A = \pm 1$ and $\det B = \pm 1$. So, $\det AB = \det A \det B = \pm 1$. So, $AB \in S$. So, S is closed under matrix multiplication. Now, I_n, the $n \times n$ identity matrix is the identity for $(GL_n(\mathbb{R}), .)$. $\det(I_n) = 1$, hence $I_n \in S$. If $A \in S$, $\det(A^{-1}) = \frac{1}{\det A} = \pm 1$. So $A^{-1} \in S$. Hence, S is a subgroup of $(GL_n(\mathbb{R}), .)$. □

Problem 4. Is the set $S = \{A \in GL_n(\mathbb{R}) | A^T A = I_n\}$ a subgroup of $(GL_n(\mathbb{R}), .)$? If yes, prove it. If not, explain why not.

Proof. Let $A, B \in S$. Then, $A^T A = I_n$ and $B^T B = I_n$. Now, $(AB)^T AB = B^T A^T AB = B^T (A^T A) B = B^T I_n B = B^T B = I_n$. So, $AB \in S$. So, S is closed under matrix multiplication. Now, I_n, the $n \times n$ identity matrix is the identity for $(GL_n(\mathbb{R}), .)$. $I_n^T I_n = I_n$, hence $I_n \in S$. If $A \in S$, $A^{-1} = A^T$. So $AA^T = I_n$. Now, $(A^{-1})^T A^{-1} = (A^T)^T A^T = AA^T = I_n$. So, $A^{-1} \in S$. Hence, S is a subgroup of $(GL_n(\mathbb{R}), .)$. □

Problem 5. Find the order of the cyclic subgroup generated by the given element.
(a) The subgroup of $(\mathbb{Z}_4, +)$ generated by 3.
(b) The subgroup of $(GL_2(\mathbb{R}), .)$ generated by $\begin{bmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{bmatrix}$.
(c) The subgroup of $(\mathbb{C}^\times, \times)$ generated by $(1 + i)/\sqrt{2}$.

Proof. (a) $3+3=2$, $3+3+3=1$, $3+3+3+3=0$. So, the order of 3 is 4, hence the order of the subgroup generated by 3 is 4.
(b) $A = \begin{bmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{bmatrix} = \begin{bmatrix} \cos(2\pi/3) & -\sin(2\pi/3) \\ \sin(2\pi/3) & \cos(2\pi/3) \end{bmatrix}$. So, A corresponds to rotation by an angle of $2\pi/3$. A^2 corresponds to rotation by an angle of $4\pi/3$, while A^3 corresponds to rotation by 2π, which is the same as the identity. So $A^3 = I$, but $A \neq I$ and $A^2 \neq I$. Hence the order of A is 3, and so the order of the subgroup generated by A is 3.
(c) Note that $(1+i)/\sqrt{2} = \cos(\pi/4) + i\sin(\pi/4)$. We want to find the smallest $n \geq 1$ such that $((1+i)/\sqrt{2})^n = 1$, i.e. $(\cos(\pi/4) + i\sin(\pi/4))^n = 1$. We recall the following general fact from complex numbers: For any $\theta \in \mathbb{R}$,

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta.$$

So, $((1+i)/\sqrt{2})^n = \cos(n\pi/4) + i\sin(n\pi/4)$. This is equal to 1 iff $n\pi/4$ is a multiple of 2π, i.e. n is a multiple of 8. Since we are interested only in the smallest $n \geq 1$ that satisfies this, we have $n = 8$. Hence the order of $(1+i)/\sqrt{2}$ is 8, and so the order of the subgroup generated by $(1+i)/\sqrt{2}$ is 8. □

Problem 6. If H and K are subgroups of an abelian group G, show that

$$\{hk | h \in H, k \in K\}$$

is a subgroup of G.

Proof. Let us denote by S the subset defined above. Let $h_1k_1, h_2k_2 \in S$. Then, since G is abelian, $h_1k_1h_2k_2 = (h_1h_2)(k_1k_2)$, which is in S. So, S is closed under the binary operation. Let e denote the identity of G. Since H and K are subgroups of G, $e \in H$ and $e \in K$. But, $e = ee \in S$. Now, let $h \in H$ and $k \in K$. Since H and K are subgroups of G, $h^{-1} \in H$ and $k^{-1} \in K$. Now $(hk)^{-1} = k^{-1}h^{-1}$. Since G is abelian, $k^{-1}h^{-1} = h^{-1}k^{-1} \in S$. So, $(hk)^{-1} \in S$. So, S is a subgroup of G. □

Problem 7. For sets H and K, define the intersection $H \cap K$ to be

$$H \cap K = \{x | x \in H \text{ and } x \in K\}.$$

Show that if H and K are subgroups of a group G, then $H \cap K$ is a subgroup of G.

Proof. Let $x, y \in H \cap K$. Then $x, y \in H$ and so $xy \in H$ as H is a subgroup of G. Similarly, $xy \in K$. So, $xy \in H \cap K$. So, $H \cap K$ is closed under the binary operation. Since $e \in H$ and $e \in K$, we also have $e \in H \cap K$. Let $x \in H \cap K$. Then $x \in H$, and so $x^{-1} \in H$. Similarly, $x^{-1} \in K$. So, $x^{-1} \in H \cap K$. So, $H \cap K$ is a subgroup of G. □

Problem 8. Find all subgroups of the given group.
(a) $\mathbb{Z}_{12}$
(b) $\mathbb{Z}_{36}$

Proof. (a) The distinct subgroups (other than $\{0\}$) of $\mathbb{Z}_{12}$ are generated by the distinct divisors of 12. So, they are $\{0\}, \{0,2,4,6,8,10\}, \{0,3,6,9\}, \{0,4,8\}, \{0,6\}$ and $\mathbb{Z}_{12}$.
(a) The distinct subgroups (other than $\{0\}$) of $\mathbb{Z}_{36}$ are generated by the distinct divisors of 36. So, they are $\{0\}, \{0,2,4,6,8,10,12,14,16,18,20,22,24,26,28,30,32,34\}$,
$\{0,3,6,9,12,15,18,21,24,27,30,33\}, \{0,4,8,12,16,20,24,28,32,36\}, \{0,6,12,18,24,30\}$,
$\{0,9,18,27\}, \{0,12,24,36\}, \{0,18\}$ and $\mathbb{Z}_{36}$. □

Problem 9. Let a and b be elements of a group G. Show that if ab has finite order n, then ba also has order n.

Proof. Since order of ab is n, we have $(ab)^n = e$ where e denotes the identity of G. Note that $(ab)^n = ababab....ab(n \text{ times}) = a(ba)^{n-1}b$. So, we have $a(ba)^{n-1}b = e$. Multiplying both sides by b on the left side, we get $(ba(ba)^{n-1})b = b$ .Canceling out b by the cancellation property, we get $(ba)^n = e$. Hence the order of ba is $\leq$ the order of ab. Applying the same argument starting with ba, we get that the order of ab is $\leq$ the order of ba. Hence the orders of both ab and ba are the same, which is n in this case.

□

Problem 10. Let p and q be distinct prime numbers. Find the number of generators of the cyclic group $\mathbb{Z}_{pq}$.

Proof. Let $0 \leq n < pq$. Then n generates $\mathbb{Z}_{pq}$ if and only if $\gcd(n, pq) = 1$. Now, for $0 \leq n < pq$ to have $\gcd(n, pq) > 1, n$ has to be either a multiple of p or a multiple of q, and hence n could be $0, p, 2p..., (q-1)p$ or $0, q, 2q, ..., (p-1)q$. Counting these, we see that there are $p + q - 1$ choices for n with $0 \leq n < pq$ and with $\gcd(n, pq) > 1$. So, there are $pq - (p + q - 1) = (p-1)(q-1)$ choices of n with $0 \leq n < pq$ and $\gcd(n, pq) = 1$. So there are $(p-1)(q-1)$ generators for $\mathbb{Z}_{pq}$. □