Problem Set 1 solutions

Problem 1. Prove that every group of order 4 is abelian, using only use the definition of a group.
Proof. Let G be a group with 4 elements, and suppose there are elements $a, b \in G$ such that $ab \neq ba$ for some elements $a, b \in G$. Let e denote the identity element of G. Since $ab \neq ba$, we must have $a \neq b$, $a \neq e$, and $b \neq e$. Since G has only 4 elements and $ab \neq ba$, either $ab \in \{e, a, b\}$ nor $ba \in \{e, a, b\}$. Without loss of generality, let us assume that $ab = e$. But $ab = e$ implies $b = a^{-1}$, and we know a^{-1} commutes with a, and hence this is not possible. If $ab = a$, then $b = e$ and if $ab = b$ then $a = e$, both of which are impossible. Since a and b were arbitrary elements, G must be abelian. □

Problem 2. Let G be a group and $x \in G$ any element. Recall that $|x|$ denotes the *order* of x, defined to be the least integer $n \geqslant 1$ such that $x^n = e$; if no such integer exists, we say $|x| = \infty$. Also, let $|G|$ denote the cardinality of G; note that $|G|$ is an element of $\{1, 2, 3, \cdots\} \cup \{\infty\}$.

(a) Prove that if $|x| = n$, then $e, x, \ldots, x^{n-1}$ are all distinct elements of G.

Proof. If $e = x^0, x, x^2, \ldots, x^{n-1}$ are not all distinct, then $x^i = x^j$ for some $0 \leqslant i < j \leqslant n-1$, and thus $x^{j-i} = e$. Since $0 < j - i < n$, this contradicts the minimality of n. □

(b) Prove that if $|x| = \infty$, then $x^i \neq x^j$ for all positive integers $i \neq j$.

Proof. Suppose $x^i = x^j$ for some $i < j$. Multiplying by the inverse of x on the right gives $x^{j-i} = e$ and $j - i > 0$, contradicting the assumption that $|x| = \infty$. □

(c) Conclude that $|x| \leqslant |G|$ in all cases.

Proof. If $|x| = n$, then part (a) shows that G contains n distinct elements, and thus $|G| \geqslant n$. If $|x| = \infty$ then part (b) shows that G has infinitely many distinct elements, and thus $|G|$ is infinite. In either case, we have $|x| \leqslant |G|$. □

Problem 3. A group G is called *cyclic* if it is generated by a single element.

(a) Prove that any cyclic group is abelian.

Note: your proof will be very short, as you can use the fact that $x^i x^j = x^{i+j}$ without proof.

Proof. Let G be a cyclic group. Then there is some element x of G such that $G = \{x^i \mid i \in \mathbb{Z}\}$. To show G is abelian, it suffices to show that $x^i x^j = x^j x^i$ for all integers i and j. But this holds because $x^i x^j = x^{i+j} = x^{j+i} = x^j x^i$, which is known as the law of exponents. □

(b) Prove that $(\mathbb{Q}, +)$ is not a cyclic group.

Proof. If $\mathbb{Q}$ is cyclic, let $\frac{a}{b}$ be a generator, so that in additive notation $\mathbb{Q} = \{\frac{ma}{b} \mid m \in \mathbb{Z}\}$. Note that $a, b \neq 0$ are integers. Now $\frac{a}{2b} \in \mathbb{Q}$, so $\frac{a}{2b} = \frac{ma}{b}$ for some $m \in \mathbb{Z}$. But in $\mathbb{Q}$ we can now divide by $\frac{a}{b}$, concluding that $m = \frac{1}{2}$, which is a contradiction since $\frac{1}{2} \notin \mathbb{Z}$. Thus $\mathbb{Q}$ is not cyclic. □

(c) Prove that $\mathrm{GL}_2(\mathbb{Z}_2)$ is not cyclic.

Proof. By (a), it suffices to prove $\mathrm{GL}_2(\mathbb{Z}_2)$ is not abelian. Let

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Since $\det(A) = \det(B) = 1$, both matrices are in $\mathrm{GL}_2(\mathbb{Z}_2)$. But $AB \neq BA$. □

Problem 4. For $n \geqslant 2$, prove that S_n is generated by (12) and the n-cycle $(12\cdots n)$.
Note: If you are unsure which formulas about permutations require proof, please ask.

Proof. Note: In all calculations below, everything should be read modulo n.

Let $H = \langle (12), (12\cdots n) \rangle$ be the group generated by (12) and $(12\cdots n)$. Since every permutation can be written as a product of transpositions, it suffices to show that every transposition is in H. We will use two useful formulas about permutations:

$$\begin{aligned} \text{F1}: \quad & (12\cdots n)(i\ \ i+1)(12\cdots n)^{-1} = (i+1\ \ i+2). \\ \text{F2}: \quad & (ij) = (1j)(1i)(1j). \end{aligned}$$

First, let us prove that $H = S_n$ using F1 and F2. Since (12) and $(12\cdots n)$ are both in H, using F1 repeatedly gives us $(i\ \ i+1) \in H$ for all i. Now take $j = i+1$ in F2, which gives us

$$\text{F3}: (i\, i+1)(1i)(i\, i+1) = (1\, i+1).$$

Since $(1\ 2) \in H$ and $(i\ i+1) \in H$ for all i, repeated applications of F3 give us $(1\ j) \in H$ for all j. Finally, since $(1\ i), (1\ j) \in H$ for all i, j, then by F2 we conclude that $(i\ j) \in H$. This shows all transpositions are in H, and thus $H = S_n$.

Let us finish the proof by checking that F1 and F2 hold. To show F1, we see that

$$\left((12\cdots n)(i\ \ i+1)(12\cdots n)^{-1}\right)(i+1) = \left((12\cdots n)(i\ \ i+1)\right)(i) = (12\cdots n)(i+1) = i+2.$$
$$\left((12\cdots n)(i\ \ i+1)(12\cdots n)^{-1}\right)(i+2) = \left((12\cdots n)(i\ \ i+1)\right)(i+1) = (12\cdots n)(i) = i+1.$$

Moreover, if $j \notin \{i, i+1\}$, then

$$\left((12\cdots n)(i\ \ i+1)(12\cdots n)^{-1}\right)(j) = \left((12\cdots n)(i\ \ i+1)\right)(j-1) = j.$$

This shows F1. To prove F2, note that

$$\left((1j)(1i)(1j)\right)(i) = \left((1j)(1i)\right)(i) = (1j)(1) = j.$$
$$\left((1j)(1i)(1j)\right)(j) = \left((1j)(1i)\right)(1) = (1j)(i) = i.$$

Moreover, if $l \notin \{i, j\}$, then $(1i)$ and $(1j)$ both keep l invariant, and thus

$$\left((1j)(1i)(1j)\right)(l) = l.$$

We conclude that F2 holds. $\square$

Problem 5. Suppose the cycle type of $\sigma \in S_n$ is $m_1, m_2, \ldots, m_k$. Recall this means that σ a product of disjoint cycles of lengths $m_1, m_2, \ldots, m_k$. Prove that $|\sigma| = \operatorname{lcm}(m_1, \ldots, m_k)$.

Proof. We first consider the case when $k = 1$; that is, we will first show the order of an m-cycle is m. Given an m-cycle $\alpha = (i_1\, i_2\, \cdots, i_m)$, note that for any k, we have $\alpha^k(i_j) = i_{j+k \pmod m}$. It follows that $\alpha^m = e$ and, for each $1 \leqslant k < m$, $\alpha^k \neq e$; hence $|\alpha| = m$.

Now we consider the general case. Assume $g_1, \ldots, g_k$ are pairwise disjoint cycles, with g_i a cycle of length m_i, and let $g := g_1 \cdots g_m$. Since these elements $g_1, \ldots, g_j$ are disjoint cycles, and disjoint cycles commute, we have $(g_1 \ldots g_k)^m = g_1^m \cdots g_k^m$ for all m. It follows that if m is a multiple of $|g_i| = m_i$ for each i, then $g_i^m = (g_i^{m_i})^{\frac{m}{m_i}} = e$, and thus $g^m = e$. In particular, $g^{\operatorname{lcm}(m_1, \ldots, m_k)} = e$.

Now suppose $1 \leqslant m < \operatorname{lcm}(m_1, \ldots, m_k)$. We need to prove that $g^m \neq e$. Note that m is not a multiple of m_i for at least one value of i; for notational simplicity and without loss of generality (since we can always renumber the list of cycles), let us assume m_1 does not divide m. Then

$$g_1^m = g_1^{m \pmod{m_i}} \neq e.$$

Thus there is an integer i with $1 \leqslant i \leqslant n$ such that $g_1^m(i) \neq i$. But since the cycles are disjoint, $g_j(i) = i$ for all $j \geqslant 2$ and hence also $g_j^m(i) = i$ for all such j. This proves that $g^m = g_1^m \cdots g_k^m$ does not fix i and thus cannot be the identity element. $\square$