Solutions

1. (10 points) Use the method of induction to prove the statement below.

   For all integers $n \geq 1$,

   $$1 \cdot 2 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + n \cdot 2^n = (n-1) \cdot 2^{n+1} + 2.$$

   Proof: We proceed by induction on n.

   Base Case: When $n = 1$, the statement is $1 \cdot 2 = (0)2^2 + 2$, which is true. So the base case holds.

   Inductive Case: Suppose that $\sum_{i=1}^{n} i \cdot 2^i = (n-1)2^{n+1} + 2$ for some $n \geq 1$.

   We need to show that

   $$\sum_{i=1}^{n+1} i \cdot 2^i = (n)2^{n+2} + 2.$$

   Observe

   $$\begin{aligned}
   \sum_{i=1}^{n+1} i \cdot 2^i &= \sum_{i=1}^{n} i \cdot 2^i + (n+1)2^{n+1} \\
   &= ((n-1)2^{n+1} + 2) + (n+1)2^{n+1} && \text{by the Ind. Hyp.} \\
   &= (2n)2^{n+1} + 2 && \text{collecting like terms} \\
   &= (n)2^{n+2} + 2,
   \end{aligned}$$

   which is what we wanted to prove.

   Observe that the formatting in this solution is trivial to do by hand. There is no reason not to write solutions in this manner.

2. (10 points) Suppose a, b, and c are nonzero integers. Prove that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

   Proof: Suppose a, b, and c are nonzero integers.
   (Show $\Longrightarrow$.) Suppose that $\gcd(a, bc) = 1$.Then there exist integers s and t such that

   $$as + bct = 1.$$

   Let d be a common divisor of a and b, say d. Since $d|a$ and $d|b$, it follows that $d|(as + bct)$. Thus, $d|1$ and we conclude that $gcd(a, b) = 1$. A cut-and-paste argument implies $gcd(a, c) = 1$.

   (Show $\Longleftarrow$.) Suppose that $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$. Then there exist integers q, r, s, and t such that

   $$qa + rb = 1 \text{ and } sa + tc = 1.$$

   By multiplying the expressions above, we obtain:

   $$1 = (qa + rb)(sa + tc) = a(qsa + qtc + rbs) + (rt)(bc) = ak_1 + (bc)k_2,$$

   where k_1 and k_2 are integers.

   Let d be a common divisor of a and bc, say d. Since $d|a$ and $d|bc$, it follows that $d|(ak_1 + (bc)k_2)$. Thus, $d|1$ and we conclude that $gcd(a, bc) = 1$.

3. (25 points) Give an examples of the following, if they exist. Otherwise briefly explain why such examples do not exist.

   (a) An infinite nonabelian group.
   The set of 2×2 nonsingular matrices under the operation of matrix multiplication.

   (b) An abelian group of order n for any integer n, $n \geq 1$.
   The set of integers under addition modulo n.

   (c) A group G with exactly two subgroups.
   The set of integers under addition modulo p where p is a prime.

   (d) An infinite cyclic group.
   The set of integers under addition are generated by the element 1.

   (e) A nonabelian group such that every proper subgroup is abelian.
   The set of symmetries of a triangle (i.e. S_3) or $U(8)$ are examples we have seen in class.

4. (25 points) Let $\sigma = (12345)$, $\tau = (2436)$, and $\rho = (123)(24)(264)(45)$ be elements of S_6, the symmetric group on 6 letters.

   (a) Find $\sigma \circ \tau(2)$ and $\tau \circ \sigma(2)$.

   $\sigma \circ \tau(2) = \sigma(4) = 5; \quad \tau \circ \sigma(2) = \tau(3) = 6$

(b) Determine $|\sigma|$, the order of σ in S_6.

Since σ is a 5-cycle, its order is 5. (That is $\sigma^5 = ()$.)

(c) Write ρ as a product of disjoint cycles.

$\rho = (45)(1263)$

(d) Write ρ as a product of transpositions.

Using the answer from (c), we get $\rho = (45)(13)(16)(12)$

(e) Write $(\sigma \circ \tau)^{-1}$ as a product of disjoint cycles.

$(\sigma \circ \tau)^{-1} = \tau^{-1}\sigma^{-1} = (6342)(54321) = (152)(36)$

5. (15 points)

(a) State the definition of a group.
A group is a set G along with a binary operation $\circ$ on G (ie $\circ : G \times G \to G$) such that

(i) $\forall a,b,c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$
(ii) $\exists e \in G$ such that $\forall a \in G$, $a \circ e = e \circ a = a$.
(iii) $\forall a \in G$, $\exists a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a \in G$.

(b) Let X be the set of bijections from $\mathbb{R}$ to $\mathbb{R}$. Show that the set X under the operation of function composition is a group.

Proof:
(Show X is a binary operation under $\circ$.) Let $f,g \in X$. Since both f and g map $\mathbb{R}$ to $\mathbb{R}$, we know $f \circ g$ maps $\mathbb{R}$ to $\mathbb{R}$. Since the composition of two bijections is itself a bijection, we know $f \circ g$ is a bijection. Thus, $f \circ g \in X$.

(Show $(X, \circ)$ is associative.) We know that the composition of functions is associative provided the operations is defined.

(Show there exists an identity.) Let $e = e(x) = x$. Since e is a bijection from $\mathbb{R}$ to $\mathbb{R}$ we know $e \in X$. Let $f(x) \in X$. Observe that $(f \circ e)(x) = f(e(x)) = f(x)$ and $(e \circ f)(x) = e(f(x)) = f(x)$. So X has an identity.

(Show there exists an identity.) Let $f(x) \in X$. Since $f(x)$ is a bijection from $\mathbb{R}$ to $\mathbb{R}$, we know it has an inverse, $f^{-1}(x)$ that is also a bijection from $\mathbb{R}$ to $\mathbb{R}$. Thus, $f^{-1}(x) \in X$.

6. (15 points) Short Answer

   (a) Determine the order of the element 3 in the group $(\mathbb{Z}_{18},+)$, the integers under addition modulo 18 and find the inverse of 3.
   The identity here is 0. So the inverse of 3 is 15 since $3+15\equiv 0\,(\text{mod}18)$.
   The order of 3 is 6 since $(3+3+3+3+3+3)=18\equiv 0\,(\text{mod}18)$ and $k\cdot 3\not\equiv 0\,(\text{mod}18)$ for any k smaller than 6.

   (b) Identify the elements of $U(9)$, determine the order of 4, and identify the inverse of 4.
   $U(9)=\{1,2,4,5,7,8\}$. The operation is multiplication modulo 9 and identity here is 1. We claim the order of 4 is 3 because $4^1=4$, $4^2=16\equiv 7(\text{mod}9)$, and $4^3\equiv 1(\text{mod}9)$. The previous calculation also shows that the inverse of 4 is 7.

   (c) Let a be an element of G, a group. If $a^{12}=e$, what are the possible orders of a?

   The order a has to divide 12. So the order of a is one of: 1,2,3,4,6,12.

7. (5 points Extra Credit) Prove that if G is a group such that for every $x,y\in G$, $xy=x^{-1}y^{-1}$, then G is abelian.

   Proof: Suppose that G is a group such that for every $x,y\in G$, $xy=x^{-1}y^{-1}$.

   Observe that by assumption $x=x\cdot e=x^{-1}e^{-1}=x^{-1}$. (That is, the hypothesis implies that every element is its own inverse.) Since every element is its own inverse, we know $xy=(xy)^{-1}=y^{-1}x^{-1}$.
   But now we have $y^{-1}x^{-1}=xy=x^{-1}y^{-1}$. (We are really done here since every element is the inverse of some other element. However, if you are not comfortable with this, you could go further as follows.)

   Take the expression $y^{-1}x^{-1}=x^{-1}y^{-1}$ and operate on the left and the right by y to obtain: $x^{-1}y=yx^{-1}$. Now operate on the left and right by x to obtain: $yx=xy$.