HW2

Please type or photograph your solution and turn it into a pdf before submitting it to Canvas. The first two problems will be graded for correctness.

1. Let A be a set. $+_A : P(A) \times P(A) \to P(A)$ defined as $(B, C) \mapsto (B \cup C) \backslash (B \cap C)$. Then:
   (a) Show that $(P(A), +_A)$ is an abelian group.
   (b) Let $A' \subseteq A$, show that $B \mapsto B \cap A'$ is a homomorphism from $(P(A), +_A)$ to $(P(A'), +_{A'})$.
   (c) Let $F = \{B \in P(A) : B \text{ is finite or } A \backslash B \text{ is finite}\}$. Show that F is a subgroup of $(P(A), +_A)$.

2. Let G be a group, H_1, H_2 be two subgroups.
   (a) Show that $H_1 \cap H_2 \leq G$.
   (b) Show that $H_1 \cup H_2 \leq G$ iff $H_1 \leq H_2$ or $H_2 \leq H_1$.
   (c) Let G be the group of integers and the group operation is addition. Write down two subgroups whose union is no longer a subgroup.

3. Show that the set of $n \times n$ matrices with integer entries and determinant 1 form a group under matrix multiplication. (These groups are denoted as $SL(n, \mathbb{Z})$.

4. Let G be a group, show that G has only the identity element iff for any group H, $Hom(H, G)$ has exactly one element.

5. Show that for any group G, any $g \in G$, there is a unique group homomorphism from $(\mathbb{Z}, +)$ to G, sending 1 to g.

6. Let M be a set, $* : M \times M \to M$ be a function, such that for any $a, b, c \in M$, $*(a, *(b, c)) = *(*(a, b), c)$, $*(a, b) = *(b, a)$, and there is an element $e \in M$ such that for any $a \in M$, $*(e, a) = *(a, e) = a$. Let $\cdot : (M \times M) \times (M \times M) \to M \times M$ be $((a, b), (c, d)) \mapsto (*(a, c), *(b, d))$, $\sim$ a relation on $M \times M$ defined as $\sim = \{((a, b), (c, d)) \in (M \times M) \times (M \times M) : \text{ there exists } k \in M, *(*(a, d), k) = *(*(b, c), k)\}$
   (a) Show that $\sim$ is an equivalence relation.
   (b) Let $G = (M \times M)/\sim$. Show that $([a], [b]) \mapsto [\cdot(a, b)]$ is a function from $G \times G$ to G. Denote it as $\cdot'$.

(c) Show that $(G, \cdot')$ is an abelian group. This is called the Grothendieck group of $(M, *)$.

(d) Show that there is a bijective homomorphism from the Grothendieck group of $(\mathbb{Z}\backslash\{0\}, \times)$ to the group $(\mathbb{Q}\backslash\{0\}, \times)$.

Answer:

1. (a) $+_A$ is clearly well defined, and from definition one can see that $B +_A C = C +_A B$ for any $B, C \in P(A)$.

    i. Associativity: if $B, C, D \in P(A)$, $a \in A$ lies in $B +_A C$ iff a is in B or C but not both, hence a is in $(B +_A C) +_A D$ iff a is in B but not C or D, C but not B or D, D but not B or C, or in all three sets B, C and D. Similarly $a \in B +_A (C +_A D)$ can be shown to have the same meaning, hence $(B +_A C) +_A D = B +_A (C +_A D)$.

    ii. Identity element is $\emptyset$, because $(\emptyset \cup B)\backslash(\emptyset \cap B) = B\backslash\emptyset = B$.

    iii. The inverse of $B \in P(A)$ is the element B itself.

    These show that $(P(A), +_A)$ is an abelian group.

   (b) Denote this map as r, then for every $B, C \in P(A)$, $r(B) +'_A r(C) = ((B \cap A') \cup (C \cap A'))\backslash((B \cap A') \cap (C \cap A')) = ((B \cup C\backslash(B \cap C)) \cap A' = r(B +_A C)$.

   (c) Clearly $\emptyset \in F$. If $B \in F$, because $-B = B$, $-B \in F$, hence F is closed under inverse. To show that F is closed under group operation, suppose $B, C \in F$. Then there are three cases:

    i. Both B and C are finite, then $B +_A C \subseteq B \cup C$ is finite hence in F.

    ii. Both $A\backslash B$ and $\backslash C$ are finite, then $B +_A C = (B +_A (A +_A A)) +_A (C +_A (A +_A A)) = ((B +_A A) +_A A) +_A ((C +_A A) +_A A) = (A\backslash B) +_A (A\backslash C) \subseteq (A\backslash B) \cup (A\backslash C)$ is finite, hence in F.

    iii. B or C is finite, and the complement of the other is finite as well. Suppose B and $A\backslash C$ are both finite, then $A\backslash(B +_A C) = A +_A (B +_A C) = B +_A (A +_A C) = B +_A (A\backslash C) \subseteq B \cup (A\backslash C)$ is finite, hence $B +_A C \in F$.

2. (a) Let i be the inclusion map from H_1 to G, then $H_1 \cap H_2 = i^{-1}(H_2)$, hence $H_1 \cap H_2 \leq H_1$. Because the group operation on H_1 is the restriction of the group operation on G, $H_1 \cap H_2$ is non-empty and closed under this group operation and inverse, hence is a subgroup of G.

   (b) If $H_1 \leq H_2$ or $H_2 \leq H_1$, $H_1 \cup H_2 = H_2$ or H_1, hence is a subgroup of G. On the other hand, if neither $H_1 \leq H_2$ nor $H_2 \leq H_1$, there are $a \in H_1\backslash H_2$ and $b \in H_2\backslash H_1$. Suppose $H_1 \cup H_2 \leq G$, then $ab \in H_1 \cup H_2$. If $ab \in H_1$, then $b = a^{-1}(ab) \in H_1$, a contradiction. If $ab \in H_2$, then $a = (ab)b^{-1} \in H_2$, also a contradiction.

   (c) By (b) above, we can pick for example $\langle 2 \rangle$ and $\langle 3 \rangle$.

3. (a) The product of two integer matrices has integer entries, and the determinant equals the product of their determinant, hence matrix multiplication is a well defined function from $SL(n, \mathbb{Z}) \times SL(n, \mathbb{Z})$ to $SL(n, \mathbb{Z})$.

   (b) Associativity follows from the associativity of matrix multiplications.

   (c) The identity element is the identity matrix $I_n \in SL(n, \mathbb{Z})$.

   (d) By Cramer's rule, the inverse of a matrix is $\frac{1}{det}$ times the matrix of cofactors. If $A \in SL(n, \mathbb{Z})$, $\frac{1}{\det(A)} = 1$, and the matrix of cofactors is an integer matrix, hence A^{-1} is an integer matrix. $det(A^{-1}) = 1/det(A) = 1$, hence $A^{-1} \in SL(n, \mathbb{Z})$.

4. If G has only the identity, the only map from H to G must be the constant map sending everything to the identity, which is a group homomorphism. If G has more elements than the identity, $Hom(G, G)$ has at least two elements, one being the identity map $g \mapsto g$, one being the constant map $g \mapsto e$.

5. It is easy to check that the map $f(n) = \begin{cases} g^n & n > 0 \\ e & n = 0 \\ (g^{-n})^{-1} & n < 0 \end{cases}$ is such a group homomorphism. To show that it is unique, if f' is a homomorphism sending 1 to g, then if $n > 0$, $f'(n) = f'(1+1+\cdots+1) = f'(1)f'(1)\ldots f'(1) = f'(1)^n = g^n$, and if $n < 0$ then $f'(-(-n)) = f'(-n)^{-1} = (g^{-n})^{-1}$, hence $f' = f$.

6. For convenience we write $*(a, b)$ as ab

   (a) i. If $(a, b) \in M \times M$, $ab = ab$, hence $(a, b) \sim (a, b)$.

      ii. If $(a, b), (c, d) \in M \times M$, $(a, b) \sim (c, d)$, then $adk = bck$, which implies $cbk = dak$, hence $(c, d) \sim (a, b)$.

      iii. If $(a, b), (c, d), (s, t) \in M \times M$, $(a, b) \sim (c, d)$, $(c, d) \sim (s, t)$, then $adk = bck$, $ctk' = dsk'$, hence $adkctk = bckdsk'$ which implies that $at(cdkk') = bs(cdkk')$, which shows that $(a, b) \sim (s, t)$.

   (b) To show this is well defined, we only need to show the value doesn't depend on the exact choice of the representative. In other words, suppose $(a, b) \sim (a', b')$, $(c, d) \sim (c', d')$, we need to show that $(ac, bd) \sim (a'c', b'd')$. $(a, b) \sim (a', b')$, $(c, d) \sim (c', d')$ implies that $ab'k = ba'k$, $cd'k' = dc'k'$, hence $(acb'd'kk' = bda'c'kk'$ which finishes the proof.

   (c) Associativity and commutativity follows from the associativity and commutativity of M, $[(a, a)]$ is the identity element, and $[(a, b)] = [(b, a)]$.

   (d) The homomorphism can be defined as $[(p, q)] = p/q$.

i. To show that it is well defined, if $(p, q) \sim (p', q')$, then $pq'k = qp'k$, hence $p/q = p'/q'$.
ii. To show that it is an injection, $p/q = p'/q'$ implies $pq' = qp'$ which implies $(p, q) \sim (p', q')$.
iii. To show that it is a surjection, every $p/q \in \mathbb{Q}$ is the image of $[(p, q)]$.