Math 307 Abstract Algebra **Homework 2** **Sample Solution**

1. Prove that the set of all 2×2 upper triangular matrices with entries from $\mathbb{R}$ and determinant 1 is a group under matrix multiplication. Solution. Let M be the set of all 2×2 upper triangular matrices with real entries such that for $A \in M$, $\det(A) = 1$.

   (G0) Let $A = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{11} \end{pmatrix} \in M$. Then $AB = \begin{pmatrix} a_{11}b_{11} & a_{12}b_{12} + a_{12}b_{22} \\ 0 & a_{22}b_{22} \end{pmatrix}$ is an upper triangular matrix, and $\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$. Thus, $AB \in M$.

   (G1) Direct verification, or use the fact that multiplication of matrices is associative.

   (G2) Clearly, $I_2 \in M$ is the identity element satisfying $I_2 A = AI_2 = I_2$ for any $A \in M$.

   (G3) Suppose $A = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} \in M$. Then $A^{-1} = \begin{pmatrix} a_{22} & -a_{12} \\ 0 & a_{11} \end{pmatrix}$ such that $AA^{-1} = A^{-1}A = I_2$ and $\det(A^{-1}) = \det(A)^{-1} = 1^{-1} = 1$. Thus, every $A \in M$ has an inverse A^{-1} in M.

   Combining (G0) – (G3), we see that M is a group under matrix multiplication.

   Extra credits For $n \times n$ (G0) Suppose $A = [a_{ij}]$ and $B = [b_{ij}]$ is triangular each as determinant 1. Then for any $i > j$, the (i, j) entry of $AB = a_{i1}b_{1j} + \cdots + a_{in}b_{nj} = 0$. So, AB is also a triangular matrix. Clearly, $\det(AB) = \det(A)\det(B) = 1$. So, $AB \in M$.

   (G1) By the fact that matrix multiplication is associative.

   (G2) Clearly, $I_n \in M$ is the identity.

   (G3) Suppose $A = [a_{ij}]$ is upper triangular with determinant 1. Then A is invertible, and we can apply row reduction to $[A|I_n]$ to get $[I_n|A^{-1}]$. Clearly, $[A|I_n]$ is in row echelon form already. So, the row operations applied will create an upper triangular matrix A^{-1}. Now, $\det(A^{-1}) = 1/\det(A) = 1$. So, $A^{-1} \in M$.

2. Prove that the set $U(n)$ of elements in $\mathbb{Z}_m$ relatively prime to n is a group under multiplication.

   Solution. Let $\mathbb{Z}_n = \{[0], \ldots, [n-1]\}$. (G0) If $[a], [b] \in U(n)$, then $\gcd(a, n) = 1 = \gcd(b, n)$. So, a, b has no prime factors of n in their prime factorization. Hence ab has no prime factors of n and $\gcd(ab, n) = 1$. Hence, $[a][b] = [ab] \in U(n)$.

   (G1) It is known that multiplication in $\mathbb{Z}_n$ is associative.

   Thus, for any $[a], [b], [c] \in U(n)$, we have $([a][b])[c] = [a]([b][c])$.

   (G2) Evidently, $[1] \in U(n)$ is the identity.

   (G3) For any $[a] \in U(n)$, since $\gcd(a, n) = 1$, there are integers x, y such that $ax + ny = 1$.

   Thus, $[x] \in U(n)$, and $[1] = [a][x] + [n][y] = [a][x]$. Hence, $[x] \in U(n)$ is the inverse of $[a]$.

3. Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$.

   Solution. Let G be Abelian, that is, for any $a, b \in G$, $ab = ba$. Then $(ab)^{-1} = (ba)^{-1} = a^{-1}b^{-1}$. Now suppose $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$. Then $(ab)(ab)^{-1} = e$ and $(ba)(ab)^{-1} = ba(a^{-1}b^{-1}) = e$. By cancellation, $ab = ba$.

4. Prove that in any group, an element and its inverse have the same order.

   Solution. Let G be a group and let $a \in G$.

   Case 1. Suppose $|a| = m$ is finite. Then $a^m = e$ so that $(a^{-1})^m a^m = e$. Thus, $(a^{-1})^m = e$. If $|a^{-1}| = n$, then $n \le m$ because $|b|$ is the smallest positive integer n such that $b^n = e$. If $1 \le n < m$, then $a^{m-n} = a^m (a^{-1})^n = e$, contradicting the fact that $|a| = m$. So, $m = n$.

   Next, suppose $|a|$ is infinite. If $|a^{-1}| = n$ is finite, then by the above argument $|a| = |(a^{-1}| = n$, which is a contradiction.

5. Suppose that H is a proper subgroup of $\mathbb{Z}$ under addition and H contains $18, 30$ and 40, Determine H.

   Solution. Note that $2 = 40 + 40 - 30 - 30 - 18 \in H$. So, H contains $2\mathbb{Z}$, and hence the subgroup $\langle 2 \rangle$ of all even numbers. If H contains any additional element a, it will be of the form $2k + 1$. Then $1 = (2k + 1) - 2k \in H$ and $H = \mathbb{Z}$. Hence, H cannot contain other elements, and $H = 2\mathbb{Z}$.

6. Let H_α be a subgroup of a group G for every $\alpha \in J$. Prove that $\cap_{\alpha \in J} H_\alpha$ is a subgroup of G.

   Solution. Note that for each α, $e \in H_\alpha$, we have $e \in \bigcap_{\alpha \in J} H_\alpha$. Thus, $\bigcap_{\alpha \in J} H_\alpha \neq \emptyset$.

   Let $a, b \in \bigcap_\alpha H_\alpha$. Then $a, b \in H_\alpha$ for each $\alpha \in J$. Thus, we have $ab^{-1} \in H_\alpha$.

   Hence $ab^{-1} \in \bigcap_{\alpha \in J} H_\alpha$. By Theorem 3.1, $\bigcap_{\alpha \in J} H_\alpha \le G$.

7. Let $H, K \le G$. Show that $H \cup K \le G$ if and only if $H \le K$ or $K \le H$.

   Solution. Let G be a group and let $H, K \le G$. Assume without loss of generality that $H \le K$, that is $H \subseteq K$, which implies that $H \cup K = K \le G$.

   Conversely, assume that $H \not\le K$ and $K \not\le H$. Then, there exists an $h \in H \backslash K$ and a $k \in K \backslash H$ such that $h, k \in H \cup K$, Suppose, $H \cup K$ were a subgroup of G. Then $hk \in H \cup K$.

   Case 1. If $hk \in H$, then $h^{-1} \in H$ and hence $k = h^{-1}(hk) \in H$, which is a contradiction.

   Case 2. If $hk \in K$, then $k^{-1} \in K$ and hence $h = (hk)k^{-1} \in K$, which is a contradiction.

   Thus, $H \cup K$ cannot be a subgroup.

8. Extra credits. Let G be the Klein four group consisting of the matrices

$$I_2, \quad A_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

   under matrix multiplication. Then $H_i = \{I_2, A_i\}$ is a subgroup for each $i = 1, 2, 3$, and $G = H_1 \cup H_2 \cup H_3$ is a subgroup.

   The question is not very well-stated. We can also let $(G, *) = (\mathbb{Z}, +)$, $H_1 = \{8k : k \in \mathbb{Z}\}$, $H_2 = \{4k : k \in \mathbb{Z}\}$, $H_3 = \{2k : k \in \mathbb{Z}\}$ so that $H_1 \cup H_2 \cup H_3 = H_3$ is a subgroup.