Abstract Algebra

Homework 4: 1, 5.3, 5.4, 5.14, 5.22

Kenny Roffo

Due February 20

1. Let S be the group of all 3×3 permutation matrices. Determine all of the subgroups of S. Determine which subgroups are cyclic and find a generator. Those which are not cyclic, prove whether they are abelian. (Naming of sets for reference in subgroup lattice)

$$S = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \right\}$$

This subgroup of S is neither cyclic nor abelian. Consider the counterexample

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

but commuting the matrices we see

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

Thus this subgroup of S is nonabelian.

$$S_1 = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\}$$

This subgroup of S is cyclic and abelian. It contains one element, the identity, so this is trivial.

$$S_2 = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \right\}$$

This subgroup of S is cyclic with generator $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$.

$$S_3 = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \right\}$$

This subgroup is cyclic with generator $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$.

$$S_4 = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\}$$

This subgroup is cyclic with generator $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

$$S_5 = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \right\}$$

This subgroup of S is cyclic with generator $\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$.

5.3: $SL(n, \mathbb{R})$ is the set of all $n \times n$ matrices with determinant equal to 1. Prove that $SL(n, \mathbb{R})$ is a subgroup of $GL(n, \mathbb{R})$.

Proof: $GL(n, \mathbb{R})$ is the set of all invertible $n \times n$ matrices. By the invertible matrix theorem, $GL(n, \mathbb{R})$ is the set of all $n \times n$ matrices with nonzero determinants. By definition, every element of $SL(n, \mathbb{R})$ has determinant equal to 1, which is nonzero. Therefore every element of $SL(n, \mathbb{R})$ is also an element of $GL(n, \mathbb{R})$. Thus to show $SL(n, \mathbb{R})$ is a subgroup of B we need only show it is closed under matrix multiplication and inverses. Let $A, B \in SL(n, \mathbb{R})$. From the properties of matrices, we know for an invertible matrix X that $det(X^{-1}) = \frac{1}{det(X)}$. $det(A) = 1$ so $det(A^{-1}) = \frac{1}{1} = 1$. Therefore $A^{-1} \in SL(n, \mathbb{R})$. Also, from the properties of matrices we know for matrices X, Y that $det(XY) = det(X)det(Y)$. Then $det(AB) = det(A)det(B) = (1)(1) = 1$, so $AB \in SL(n, \mathbb{R})$. Thus we have shown $SL(n, \mathbb{R})$ is closed under inverses and matrix multiplication, therefore, by definition of subgroup, $SL(n, \mathbb{R})$ is a subgroup of $GL(n, \mathbb{R})$..

5.4: Find all the subgroups of each group and sketch the corresponding subgroup lattice:

a) $(\mathbb{Z}_8, +)$:

$< 1 >= \{1, 2, 3, 4, 5, 6, 7, 0\}$
$< 2 >= \{2, 4, 6, 0\}$
$< 4 >= \{4, 0\}$
$< 0 >= \{0\}$

b) $(\mathbb{Z}_{35}, +)$:

$< 1 >= \{1, 2, 3, ..., 33, 34, 0\}$
$< 5 >= \{5, 10, 15, 20, 25, 30, 0\}$
$< 7 >= \{7, 14, 21, 28, 0\}$
$< 0 >= \{0\}$

c) $(\mathbb{Z}_{36}, +)$:

$< 1 >= \{1, 2, 3, ..., 34, 35, 0\}$
$< 2 >= \{2, 4, 6, ..., 32, 34, 0\}$
$< 3 >= \{3, 6, 9, ..., 30, 33, 0\}$
$< 4 >= \{4, 8, 16, ..., 28, 32, 0\}$
$< 6 >= \{6, 12, 18, 24, 30, 0\}$
$< 9 >= \{9, 18, 27, 0\}$
$< 12 >= \{12, 24, 0\}$
$< 18 >= \{18, 0\}$
$< 0 >= \{0\}$

5.14: Prove that the intersection of two subgroups of a group G is itself a subgroup of G.

Proof: Let H and K be subgroups of some group G. Then all elements of H and K are subsets of G which are closed under the operation of G and inverses. Since H and K are subsets of G, $H \cap K$ is also a subset of G. We must show $H \cap K$ is closed under the operation of G. Let $X, Y \in H \cap K$. Then $X, Y \in H$, and $X, Y \in K$. Since H and K are subgrouops of G, they are closed under the operation, so $XY \in H$ and $XY \in K$. Then $XY \in H \cap K$. We must show $H \cap K$ is closed under inverses. Let $X \in H \cap K$. Then $X \in H$ and $X \in K$. Since H and K are subgroups of G, they are closed under inverses, so $X^{-1} \in H$, and $X^{-1} \in K$. Since X^{-1} is in both H and K, $X^{-1} \in H \cap K$, thus $H \cap K$ is closed under inverses. We have shown $H \cap K$ is closed under the operation of G and inverses, thus we have shown $H \cap K$ is a subgroup of G.

5.22: Let G be a group. Prove that $Z(G)$ is a subgroup of G.

Proof: $Z(G)$ is the subset of elements z in G for which $zx = xz$ for all $x \in G$. Since G is a group, the operation, $*$, in on G is an associative binary operator. Also, the identity, e is an element of $Z(G)$ since the identity of a group is commutative by definition of a group. Thus to prove $Z(G)$ is a group we must show $Z(G)$ is closed under * and inverses. Let $w, z \in Z(G)$ and let x be an arbitrary element of G. Then $zx = xz$ and $wx = xw$ by definition of $Z(G)$. Multiplying on the left and right sides by z^{-1}, an element of G, we have $z^{-1}zxz^{-1} = z^{-1}xzz^{-1}$, which simplifies to $xz^{-1} = z^{-1}x$. Thus z^{-1} is commutative in G, so z^{-1} satisfies the condition to be an element of $Z(G)$. Therefore inverses exist in $Z(G)$ for all elements in $Z(G)$. Also, $zwx = zxw$ (by multiplying on the left by z. Since G is a group and thus closed under its operation, $xw \in G$, so $zwx = xwz$ since $z \in Z(G)$. Now since $w \in G$, we see $wz = zw$, so $zwx = xzw$. Therefore zw is commutative with x, and arbitrary element in G. So $Z(G)$ is closed under the operation of G. Thus all of the group axioms are satisfied by $Z(G)$ so $Z(G)$ is a group. Therfore, since all elements of $Z(G)$ are elements of G, $Z(G)$ is a subgroup of G.