Math 320 Assignment 1

August 7th, 2008
Erik Born
SID#: 1072989

Question 1 Since $(G, \circ)$ is a group, $b \circ a$ is an element of the group. Thus for all $a, b \in G$ $a \star b = b \circ a \in G$. Therefore $\star$ is a binary operation on G. $(G, \star)$ is a group, because $b \star a = a \circ b$, the identity element of $(G, \circ)$ must be the same as the identity element of $(G, \star)$, since by the definition of an identity element, $a \circ e = e \circ a = a$ and by the definition of $\star$, $a \circ e = e \star a = e \circ a = a \star e = a$. The inverse characteristic for $(G, \star)$ also follows from $(G, \circ)$ because $a \circ a^{-1} = a^{-1} \circ a = e = a \star a^{-1} = a^{-1} \star a$. The associativity follows in a similar way. Since $(a \star b) \star c = (b \star a) \circ c = c \circ (b \circ a)$ and $a \star (b \star c) = a \star (c \circ b) = (c \circ b) \circ a = c \circ (b \circ a)$ since $(G, \circ)$ is a group.

Question 2
Part a)

TABLE 1. Cayley table for $G = (U(18), \times_{18})$

$\times_{18}$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

Part b)

Proof. Suppose $G = (U(18), \times_{18})$, $\forall\, a, b \in U(18)$ $a \times_{18} b = (a \times b)_{18}$. Since $a \times b = b \times a, a \times_{18} b = (a \times b)_{18} = (b \times a)_{18} = b \times_{18} a$, as required for an Abelian group. □

Part c)

TABLE 2. Order of the elements of $G = (U(18), \times_{18})$

Element	1	3	5	7	11	13	17
Order	1	6	6	6	6	6	6

G is a cyclic group, all of the elements are generators with the exception of the identity element.

Question 3
Part a) The elements in $G = D_n$ that have order two are either reflections, or the a rotation equal to 180 degrees. Every group D_n has n reflections and n rotations if you consider the identity element to be a reflection. Only groups that have an even number of sides will have a rotation symmetry equal to $R_1 80$, therefore for the number of elements in $G = D_n$ that have order two is n if the group is odd, and $n + 1$ if the group is even.

Part b)

Proof. Suppose $G = D_n$ where $n \geq 3$ and G is finite and of even order. For a symmetry group of order $2n$ there are n reflections. Each reflection when composed with itself gives the original. That is, for each reflection $\alpha, \alpha \circ \alpha = \alpha^2 = R_0 = e$. Thus for all reflections, $\alpha = \alpha^{-1}$, which means that $< \alpha >= 2$. For any n-gon , the rotations are of the form $R_x = x360/n$ for $x \in \mathbb{Z}$ with $0 \leq x \leq n - 1$. For an even n-gon when $x = n/2, R_x = 180$. For even rotations $x = n/2$ does not exist because $n/2 \notin \mathbb{Z}$. The rotation R_{180} is also an element of order 2, $R_{180} \circ R_{180} = R_{360} = R_0 = e$. Therefore for $G = D_n$ where G is finite and of even order, there are $n + 1$ elements of order two. Since n is even, $n + 1$ must be odd. □

Question 4

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in GL(2,7). \quad A^{-1} = \frac{1}{4-6}\begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} = 2^{-1}\begin{pmatrix} 4 & 5 \\ 4 & 1 \end{pmatrix} = 4\begin{pmatrix} 4 & 5 \\ 4 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 6 \\ 2 & 4 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in GL(2,5). \quad A^{-1} = \frac{1}{4-1}\begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} = 3^{-1}\begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix} = 2\begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix}$$

Question 5

Let $G =< a >$ be the cyclic group of order 40.

Part a) $H =< a^{32} >=< a^{\gcd(n,k)} >=< a^8 >$ and $| < a^8 > | = n/\gcd(n,k) = 40/8 = 5$

Part b) $G =< a^k >$ if and only if $\gcd(n,k) = 1$. Therefore the generators of G are all the numbers that are relatively prime to 40. These are $a^1, a^3, a^7, a^{11}, a^{13}, a^{17}, a^{19}, a^{23}, a^{27}, a^{29}, a^{31}, a^{33}, a^{37}$, and a^{39}.

Part c) All the elements of order 8 in $G =< a^{40/8} >=< a^5 >= \{e, a^5, a^{10}, a^{15}, a^{20}, a^{25}, a^{30}, a^{35}\}$

Part d)

TABLE 3. Subgroups of G

Generator		Elements	Order
$< a >$	=	$\{e, a, a^2, \ldots, a^{39}\}$	40
$< a^2 >$	=	$\{e, a^2, a^4, \ldots, a^{38}\}$	20
$< a^4 >$	=	$\{e, a^4, a^8, \ldots, a^{36}\}$	10
$< a^5 >$	=	$\{e, a^5, a^10, \ldots, a^{35}\}$	8
$< a^8 >$	=	$\{e, a^8, a^16, \ldots, a^{32}\}$	5
$< a^{10} >$	=	$\{e, a^{10}, a^{20}, a^{30}\}$	4
$< a^{20} >$	=	$\{e, a^{20}\}$	2
$< a^{40} >$	=	$\{e\}$	1

Question 6

Let G be the group $(SL(2,\mathbb{Z}), \times)$.

Part a) The center of $G = (SL(2,\mathbb{Z}), \times)$ is $Z(G) = \{A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} | a \in \mathbb{Z}\}$. This group is abelian, by definition of a center $xA = Ax \ \ \forall x \in G$.

Part b)

$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ $AA = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ $AAA = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ $AAAA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ Thus $|A| = 4$.

$B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ $BB = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ $BBB = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ Thus $|B|$ is 3.

$AB = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$ $(AB)(AB) = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$ $(AB)^n = (-1)^n \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ Since $(AB)^n \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$ for any $n \in \mathbb{N}$, $|AB|$ is infinite.

Part c)

Proof. Suppose G is an abelian group. Let $H \subseteq G$ is the set of elements of finite order in G. For any $a \in H, |a| = n, \exists a^{-1} \in H$ with $|a^{-1}| = |a^n a^{-1}| = |a^{n-1}| < \infty$. Suppose $a, b \in H$ and therefore $|a| = n$ and $|b| = m$. Then $(ab)^{nm} = a^{nm}b^{nm}$ since G is an abelian group. Since $(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = e^m e^n = e$ $|ab$ has order at most equal to $mn < \infty$. By the two step test $H \leq G$. □

Question 7

Part a) $\sigma = (1,7,9,10,11)(2,3,4,5,6)$

Part b) The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles. τ has cycles of lengths 4,3,2,2. Therefore the order is 12.

Part c)

$\tau^{-1} = (1,2,3,4)^{-1}(5,6,7)^{-1}(8,9)^{-1}(10,11)^{-1} = (4,3,2,1)(7,6,5)(8,9)(10,11) = (1,4,3,2)(5,7,6)(8,9)(10,11)$

Part d) $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 4 & 5 & 7 & 2 & 9 & 6 & 10 & 8 & 1 & 11 \end{pmatrix} = (1,3,5,2,4,7,6,9,8,10)$

Part e) $\sigma = (1,7,9,10,11)(2,3,4,5,6) = (1,11)(1,10)(1,9)(1,7)(2,6)(2,5)(2,4)(2,3)$. Eight disjoint cycles means that σ is even.

Part f) $(\sigma\tau)^{9002} = (\sigma\tau)^{9000}(\sigma\tau)^2 = ((\sigma\tau)^{10})^{900}(\sigma\tau)^2 = e^{900}(\sigma\tau)^2 = (\sigma\tau)^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 7 & 2 & 6 & 4 & 8 & 9 & 1 & 10 & 3 & 11 \end{pmatrix}$

Part g) For there to be a positive integer i such that τ^i has order 7 then the lowest common multiple of the lengths of the cycles would have to be 7 for some permutation. Since 7 is prime then it would have to have a factor of 7. The biggest cycle is of length 4, and since the cycles are as big as they can get and are smaller then seven, the necessary cycle of length seven will never appear, so $|\tau^i| \neq 7 \quad \forall i \in \mathbb{N}$.

Question 8

$H = (2\mathbb{Z}, +)$ is a proper subgroup of G which contains the integers 12 and -26. It is easy to see that this is a valid subgroup for G since for any $a \in H, 2|a$and $a^{-1} = -a$ and $2|(-a)$ so $(-a) \in H$. Also for all $a, b \in H2|a$ and $2|b$ thus $2|ab$ so $ab \in H$.

Question 9

Part a) $H \cup K$ must be equal to $\{e\}$ if H and K are distinct cyclic subgroups of order p of G, where p is a prime number. If $\exists c \in H$ and K then for some integers $n, m \in \mathbb{Z}$ $c = a^n = b^m$. Since H and K both have the same order, if $a^n = b^m$ for some $n, m \in \mathbb{Z}a^{np+1} = b^{mp+1} = a = b$ thus since they have the same order and the same generator,the groups are no distinct.

Part b) By the corollary to Theorem 4.4 in Gallian, in a finite group, the number of elements of order p is a multiple of $\phi(p)$. Since $\phi(p)$ is the number of numbers relatively prime to p which are less then p, and p is prime, it's the set containing all the numbers less then p, which is a total of $p - 1$.

Part c)

Proof. If $H \cup K$ was a subgroup of G then for any elements $c, d \in H \cup K \quad \exists cd \in H \cup K$. If $c = a^{p-1}$ and $d = b^{p-1}$ then $cd = a^{p-1}b^{p-1} = (ab)^{p-1} = (ab)^p(ab)^{-1} = e(ab)^{-1}$ and $(ab)^{-1} \notin H \cup K$ since there does not exist $n \in \mathbb{Z}$ such that $a^n = ab$ and there does not exist $m \in \mathbb{Z}$ such that $b^m = ab$. Therefore $H \cup K$ is not closed and is does not fulfill the criteria of a subgroup of G. □