Homework 2

Hussein Zamzami
G00737304
Math-321
Dr. David Carchedi

October 13, 2015

1

Prove that if G is a finite abelian group of odd order, then the product

Proof. ($\prod_{g\in G} g$ of every element of G is 1 (e).
Since the the order of the group is odd, a group cannot be a multiple of two, by Lagrange's Theorem, more importantly, there cannot be a subgroup of order two such as: $\{a_1, e\}$. Therefore, there are no elements which are their own inverse, otherwise there could be a subgroup of order two. Since every element must have an inverse, by the definition of groups, every element has a unique inverse. And since G is abelian, the product can be rearranged to be a product of these inverses, such that $\prod_{g\in G} g = eg_1{g_1}^{-1}g_2{g_2}^{-1}\dots g_n{g_n}^{-1}$. Naturally, all the inverse products reduce to e, by definition of inverse. This leads to $\prod_{g\in G} g = e^n$, which is just equal to e, as e times any element is the element itself. Therefore $\prod_{g\in G} g = e$. □

2 Herstein p.64, Problem 16

If G is a finite abelian group and $a_1, \dots, a_n$ are all its elements, show that $x = a_1a_2\dots a_n$ must satisfy $x^2 = e$

Proof. Assume G is a finite abelian group and x defined as above. Then $x^2 = (a_1a_2\dots a_n)^2$ There are two cases here, either G is of odd order or G is of even order. The result of the product of all the elements of G when G is of order odd is proved in the above problem to be e and $e^2 = e$, therefore what remains to be showed is when G is of even order.
Assume G a finite abelian group of even order, then, by Lagrange's Theorem, every subgroup has order that is a multiple of two and since the identity is in each subgroup, the remaining elements must each have inverses and since there are an odd number of remaining elements (as any even number minus

1 is odd), some element must be its own inverse. Therefore, at least one element in G is its own inverse. Since G is abelian, the product can, thus, be written as a product of elements that have distinct inverses and those that don't$\{a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n\}$, with the former collection potentially being empty (as in the group $\{a, e\}$) thusly, $x = e(a_1{a_1}^{-1}a_2{a_2}^{-1}\ldots a_n{a_n}^{-1})(b_1b_2\ldots b_n)$ $({a_1}{a_1}^{-1}a_2{a_2}^{-1}\ldots a_n{a_n}^{-1})$ will reduce to e, due to being a product of inverses, allowing us to rewrite the equation as such $x = e(b_1b_2\ldots b_n)$, therefore $x^2 = (e(b_1b_2\ldots b_n))^2$, which is equal to $e^2b_1^2b_2^2\ldots b_n^2$. Since these elements are all their own inverses, however, this becomes another product of inverses which reduces to e, so that $x^2 = e^2(e^n) = e(e) = e^2 = e$ □

3 Herstein p.64, Problems 9 and 10

Problem 9: In $\mathbb{Z}_{16}$ write down all the cosets of the subgroup $H = \{[0], [4], [8], [12]\}$
The cosets are: $\{\{0, 4, 8, 12\}, \{1, 5, 9, 13\}, \{2, 6, 10, 14\}, \{3, 7, 11, 15\}\}$.
Problem 10: In Problem 9, what is the index of H in $\mathbb{Z}_{16}$
index of $H = \frac{|\mathbb{Z}_{16}|}{|H|} = 16/4 = 4$.

4 Herstein p. 65, Problem 26

Let G be a group, H a subgroup of G, and let S be the set of all distinct right cosets of H in G, T the set of all left cosets of H in G. Prove that there is a $1-1$ mapping of S onto T.

Proof. Let the mapping send every left coset $gH \mapsto (gH)^{-1}$ So that the coset is sent to its own inverse. This inverse can be rewritten as Hg^{-1}, which is a right coset. This is obviously one-to-one, as every $g \in G$ can only have one inverse and onto as every element $g \in G$ has an inverse, by definition of a group. We need to show that this is a well-defined mapping from the left cosets onto the right cosets, i.e. $f(gh)$ maps to one unique element. Since $f(gH)$ maps to Hg^{-1}, which is the right coset of H generated by g^{-1}, the cosets will be the same, as the elements of H will always be multiplied by the same element g^{-1}, since every element in G has a unique inverse. Therefore, the mapping is well-defined. □

5 Herstein p.117, Problem 2

Find the cycle decomposition and order:
a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 4 & 2 & 7 & 6 & 9 & 8 & 5 \end{pmatrix}$
Decomposition: (1 3 4 2) (5 7 9) (6) (8)
Order: 12 is the least common multiple between four and three, which must divide the order by Lagrange's theorem as there is a cycle of order four and a cycle of order three in the decomposition, therefore the order is 12.

b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$
Decomposition: (1 7) (2 6) (3 5) (4)
Order: The order is 2, as it is the LCM of the decompositions.
c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 3 & 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 7 & 4 & 2 & 1 & 3 \end{pmatrix}$
Decompositions: (1 6) (2 5) (3 7) (4) Order: LCM is 2, so the order is 2.

6 Bonus Problems

6.1 Problem B Herstein, P.66, problem 36

If $a > 1$ is an integer, show that $n \mid \phi(a^n - 1)$, where ϕ is the Euler function.

Proof. The Euler function is defined by $\phi(n) = m$ such that (m,n) = 1, that is the number of relatively prime numbers to n, so $\phi(a^n - 1)$ denotes the number of relatively prime numbers to $a^n - 1$ By Euler's Theorem, we know that $a^{\phi(n)} \equiv 1 \mod n$, therefore $a^{\phi(a^n-1)} \equiv 1 \mod (a^n - 1)$ and since the order of $a^n - 1$ is n, then $a^n - 1 \equiv 0 \mod a^n - 1$ (The order cannot be greater than n and any order less than n would not include a^n, therefore the order is), therefore n divides the equivalence classes of $a^n - 1$ of numbers that are relatively prime to $a^n - 1$, then $n \mid \phi(a^n - 1)$ □

6.2 Problem C Herstein, P. 66, problem 37

In a cyclic group of order n, show that for each positive integer m that divides n, there are $\phi(m)$ elements of order m.

Proof. In a cyclic subgroup, there must exist an element that generates the whole group, as such: $\{g, g^2, g^3, \ldots, g^n\}$ with g^n being the identity. If $m = 1$, then $\phi(m) = 1$ and there is only one element with order 1, which is the identity element. If $m = n$, then $\phi(m) = \phi(n)$ and since all the generators of a subgroup of order n are coprimes of n, there are exactly $\phi(m)$ generators in the subgroup and generators all have order $n = m$. If $m \neq 1$ and $m \neq n$ and $m \mid n$. Suppose H a subgroup of the main group. Suppose H has order m, since any group of order n is generated by a coprime of n that is less than n itself, similarly any group of order m is generated by a coprime of m that is less than m. The amount of coprimes less than m in the group is given by the Euler function, therefore, there can be as many subgroups of order m as $\phi(m)$ □

6.3 Problem D Herstein, P.66, problem 38

Using the result of problem 37, show that $n = \Sigma_{m|n}\phi(m)$.

Proof. We wish to show that n = the sum of the Euler functions of all the divisors of n, including 1 and n itself. The result of problem 37 proves that for

every divisor m of n and for every group G of order n, there are exactly $\phi(m)$ subgroups of order m. And since the order of every subgroup divides n itself, every subgroup in G is a subgroup of order m for some m that divides n. And since there are n elements in G, the total amount of subgroups generated by the elements can be written as a sum of the Euler functions representing their number, $\phi(m_1) + \phi(m_2) + \cdots + \phi(m_a)$ where every m divides n. And the total sum of this summation is n, since the functions represent all the n elements in the group. $\square$