Homework 4

Hussein Zamzami
Math-321
Dr. David Carchedi
G00737304

November 11, 2015

1 Herstein Section 3.3, problem 1

Find the parity of each permutation:
a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 5 & 1 & 3 & 7 & 8 & 9 & 6 \end{pmatrix} = (12)(24)(35)(67)(78)(89)$ $sgn(\sigma) = -1^r = -1^6 = 1$ therefore parity is even
b) $(123456)(789) = (12)(23)(34)(45)(56)(78)(89)$ $sgn(\sigma) = -1^7 = -1$, therefore parity is odd
c) $(123456)(123457) = (1357)(246) = (13)(35)(57)(24)(46)$ $sgn(\sigma) = -1^5 = -1$, so parity is odd
d) $(12)(123)(45)(568)(179) = (32)(5684)(179) = (32)(56)(68)(84)(17)(79)$, $sgn(\sigma) = -1^6 = 1$, therefore parity is even

2 Herstein Section 3.3, problem 6

If $n \geq 3$, show that every element in A_n is a product of 3-cycles.

Proof. Since every element in A_n is a product of even transpositions, what we must show is that every transposition is a product of 3-cycles. Let t_1, t_2 be transpositions with $t_1 t_2$ their product, then either t_1, t_2 have no common elements in their cycles or they have one. Take the first case, then t_1, t_2 are of the form $(ab), (cd)$ and $t_1 t_2 = (dac)(abd)$. Taking the second case, then $t_1, t_2 = (ab), (ac)$ and $t_1 t_2 = (acb)$. Therefore, since the product of any two transpositions is a product of 3-cycles and every element in A_n is a product of even transpositions, then every element in A_n is a product of 3-cycles. $\square$

3 Herstein Section 2.6, problem 11

If G is a group and $Z(G)$ the center of G, show that if $G/Z(G)$ is cyclic, then G is abelian.

Proof. Assume $G/Z(G)$ is cyclic, then $G/Z(G)$ is generated by an element $x \in G =< xZ(G) >$ and any $g \in G = (xZ(G))^n = x^n Z(G)$, therefore $gZ(G) = x^n Z(G) \implies x^{n^{-1}} g \in Z(G) \implies x^{n^{-1}} g = z \in Z(G)$ therefore, $g = zx^{n^{-1^{-1}}} = x^n z$, therefore every element in G can be rewritten as $x^a z$. Now take $g, h \in G$. $gh = x^{a_1} z_1 x^{a_2} z_2 = x^{a_1} x^{a_2} z_1 z_2 = x^{a_1+a_2} z_2 z_1 = x^{a_2} x^{a_1} z_2 z_1 = x^{a_2} z_2 x^{a_1} z_1 = hg$ □

4 Herstein Section 2.7, problem 2

Let G be the group of all real-valued functions on the unit interval $[0, 1]$, where we define, for $f, g \in G$, addition by $(f + g)(x) = f(x) + g(x)$ for every $x \in [0, 1]$. If $N = \left\{f \in G | f(\frac{1}{4}) = 0\right\}$, prove that $G/N \simeq (\mathbb{R}, +)$

Proof. If we can show that there is a surjective homomorphism $\phi : G \to \mathbb{R}$ with $ker(\phi) = N$, then by the first isomorphism theorem, we are done. Take the mapping $\phi : f \mapsto f(\frac{1}{4})$, this is a homomorphism as $(f + g)(\frac{1}{4}) = f(\frac{1}{4}) + g(\frac{1}{4})$. To show this is surjective, let $y \in \mathbb{R}$ be any real number and let $f(x) = y$, then $f(\frac{1}{4}) = y$ for all real numbers. Now we need to show that $ker(\phi) = N$, i.e. $\phi(f) \mapsto 0$ iff $f(\frac{1}{4}) = 0$. Assume $\phi(f) = 0$, then, by definition of $\phi(f)$, $f(\frac{1}{4}) = 0$. Similarly, assume $f(\frac{1}{4}) = 0$, then $\phi(f) = f(\frac{1}{4}) = 0$. Therefore, $ker(\phi) = N$, therefore, by the First Isomorphism Theorem, $G/N \simeq (\mathbb{R}, +)$. □

5 Herstein Section 2.9, problem 2

If G_1 and G_2 are cyclic groups of orders m, n, respectively, prove that $G_1 \times G_2$ is cyclic iff $gcd(m, n) = 1$

Proof. ($\Rightarrow$) If G_1, G_2 are cyclic, then $\exists x \in G_1, y \in G_2$ with order m, n respectively. Now assume $L = G_1 \times G_2$ is cyclic, then $\exists (x, y) \in L$ with order mn, as $|L| = |G_1||G_2| = mn$. Assume $gcd(m, n) \neq 1$, then $lcm(m, n) \neq mn$, therefore $\exists (a, b) \in L, a \in G_1, b \in G_2$ such that $|a| = q|m, |b| = j|n$ and $qp = jk = lcm(m, n)$ for some p, k. We will show that the order of an element in L is at most $lcm(m, n)$, $(a^{qp}, b^{jk}) = (a^{q^p}, b^{j^k}) = (e_1^p, e_2^k) = (e_1, e_2)$ which is the identity in L, therefore, the order of any element $(a, b) \in L \leq lcm(m, n)$, but since we have that $gcd(m, n) > 1$, then $lcm(m, n) < mn$, so the order of any element in $L < mn$ which implies that L is not cyclic, as there is no generator, but this contradicts the assumption that L was cyclic. Therefore, L cyclic $\implies gcd(m, n) = 1$

($\Leftarrow$) assume $gcd(m, n) = 1$ and G_1, G_2 cyclic. Then $lcm(m, n) = mn$. By the above, we know the order of an element in L is at most $mn = |L|$. Take the element $(x, y) \in L$ such that $(x, y)^k = (e_1, e_2)$, we wish to show that this implies $k = mn$. Assume $\exists k, (x, y)^k = (e_1, e_2)$ then $x^k = e_1, y^k = e_2$ this implies that $x^k = x^{m^j}, y^k = y^{n^l}$ for some j, l, therefore $k = mj, k = nl$ implying that k is a common multiple of m, n, and since lcm is the smallest such number and from above, the order cannot be greater than the lcm, $k = lcm(m,n) = mn$. Therefore, $|(x,y)| = mn = |L|$, therefore L is cyclic. $\square$

6

Let $a \in \mathbb{Z}$ and define the map of sets $\sigma_a : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ $x \mapsto x^a$ prove the following:
a) σ_a is an automorphism of $\mathbb{Z}/n\mathbb{Z}$ iff $gcd(a,n) = 1$

Proof. ($\Rightarrow$) assume σ_a is an automorphism, that is it defines a bijection from $\mathbb{Z}/n\mathbb{Z}$ onto $\mathbb{Z}/n\mathbb{Z}$. Assume $gcd(a,n) \neq 1$, then $a|n$ or $n = ak$, for some $0 < k < n \in \mathbb{Z}$. $\sigma(x) = x^a = x + \cdots + x$ a times, therefore $\sigma(x) = ax$ and $x < n$, by definition of $\mathbb{Z}/n\mathbb{Z}$, therefore, $\exists x \in \mathbb{Z}/n\mathbb{Z}, \sigma(x) = ax = n \equiv 0 \text{ mod } n$ and since $\sigma(0) = a0 = 0 \equiv 0 \text{ mod } n$, therefore meaning that σ_a is not injective, which contradicts the assumption that σ_a is an automorphism.
($\Leftarrow$) assume $gcd(a,n) = 1$, if $a = 0$, then $gcd(a,n) = n$, which contradicts the assumption, so assume $a \neq 0$. First, we need to check that σ_a defines a homomorphism. $\sigma_a(xy) = (xy)^a = x^a y^a = \sigma_a(x)\sigma_a(y)$, therefore σ_1 is a homomorphism. We wish to show that σ_a is both injective and surjective from $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. For injectivity, it is sufficient to show that $ker(\sigma_a) = \{0\}$. Assume $\sigma_a(x) = 0$ then $x^a = ax \equiv 0$ mod n, which is only true when $ax = 0$ or $ax = n$, but since $a, x \in \mathbb{Z}$, this implies either $x = 0$ or that x is a divisor of (a,n) if $x = 0$, then it is in the kernel, trivially. Assume $x \neq 0$, if $x = 1$, then $a = n \implies gcd(a,n) = n$, which is a contradiction, so 1 cannot be in the kernel of σ_a, now assume $x > 1$, then $ax = n \implies a|n \implies gcd(a,n) = a$ which contradicts the assumption that $gcd(a,n) = 1$, therefore x cannot be in the kernel of σ_a if $x > 1$, therefore x is only in the kernel if $x = 0$, which implies that σ_a is injective. For surjectivity, we have to show that every element $x \in \mathbb{Z}/n\mathbb{Z}$ can be rewritten as x^a for some a and since $\mathbb{Z}/n\mathbb{Z}$ is cyclic, then $\mathbb{Z}/n\mathbb{Z}$ has a generator x with order n, such that $\mathbb{Z}/n\mathbb{Z} = (e, x^1, \ldots, x^{n-1})$ and after applying σ_a to every element of $\mathbb{Z}/n\mathbb{Z}$, $(e^a, x^a, \ldots, x^{a(n-1)}) = (e, x^{a^1}, \ldots, x^{a^{n-1}})$, which is now the cyclic group $\mathbb{Z}/n\mathbb{Z}$ generated by $< x^a >$, which also has order n, therefore $im(\sigma_a) = \mathbb{Z}/n\mathbb{Z}$ and since σ_a is both injective and surjective, it defines an automorphism from $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. $\square$

b) For two integers, a, b $\sigma_a = \sigma_b$ iff $a \equiv b \text{ mod } n$.

Proof. ($\Rightarrow$) Assume $\sigma_a = \sigma_b$, then $\sigma_a(x) = \sigma_b(x) \forall x \in \mathbb{Z}/n\mathbb{Z} \implies x^a = x^b \implies ax = bx \implies a = b$, therefore $a \equiv b$ mod n
($\Leftarrow$) Assume $a \equiv b$ mod n, then $n = aq + b$, by Euclid's division algorithm $\square$

c) Every automorphism of $\mathbb{Z}/n\mathbb{Z}$ is equal to σ_a for some a.

Proof. Assume $\psi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defines an automorphism, then ψ has to be both injective and surjective. For ψ to be surjective, $im(\psi)$ be the whole of $\mathbb{Z}/n\mathbb{Z}$, therefore ψ maps every element x to exactly one element in $\mathbb{Z}/n\mathbb{Z}$, but every element in $\mathbb{Z}/n\mathbb{Z}$ can be represented as x^a, for some generator $x \in \mathbb{Z}/n\mathbb{Z}$ and some a, therefore $\psi : x \mapsto x^a$, which is equal to σ_a. $\square$

d) There is an explicit isomorphism of groups $U_n = (\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$

Proof. Let $\psi : (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ be the map $\psi : a \mapsto \sigma_a$. First, we wish to show this map defines a homomorphism. $\psi(ab) = \sigma_{ab} = x^{ab} = x^a x^b = \psi(a)\psi(b)$. Now to show that this is injective, we will show that its kernel is trivial, i.e. $ker(\psi) = \{1\}$, the multiplicative identity. Now, assume $\psi(a) = \sigma_a : x \mapsto x$, the identity mapping of $\mathbb{Z}/n\mathbb{Z}$, then $\sigma_a(x) = x^a = x \implies a = 1$, therefore if $a \in ker(\psi)$, then $a = 1$. Now take $\psi(1) = \sigma_1 : x \mapsto x^1 = x$, which is the identity map, therefore if $a = 1$, it is in $ker(\psi)$, which implies that $ker(\psi) = 1$, therefore ψ is injective. Now we need to show that ψ is surjective, which follows from part a), as σ_a is an automorphism iff a, n are relatively prime and $\mathbb{Z}/n\mathbb{Z}^\times$ is the set of numbers relatively prime to n. Furthermore, an inverse mapping of ψ is given by $\psi^{-1} : \mathrm{Aut}\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}^\times$ as the map $\psi^{-1} : \sigma_a \mapsto a$ and $\psi\psi^{-1} : \mathbb{Z}/n\mathbb{Z}^\times \to \mathbb{Z}/n\mathbb{Z}^\times$ is the map: $\psi\psi^{-1} : \sigma_a \mapsto a \mapsto \sigma_a$, which is the identity mapping. Therefore $\mathbb{Z}/n\mathbb{Z}^\times \xrightarrow{\sim} \mathrm{Aut}\ \mathbb{Z}/n\mathbb{Z}$ by the isomorphism $\psi : \mathbb{Z}/n\mathbb{Z}^\times \xrightarrow{\sim} \mathrm{Aut}\ \mathbb{Z}/n\mathbb{Z}$, which maps $\psi : a \mapsto \sigma_a$. $\square$

7 Bonus Problems

7.1 A

7.2 B

7.3 C