Dr. Marques Sophie
Office 519

Algebra 1

Spring Semester 2015

marques@cims.nyu.edu

Midterm

The grader cannot be expected to work his way through a sprawling mess of identities presented without a coherent narrative through line. If he can't make sense of it in finite time you could lose coherent narrative through line. If he can't make sense of it in finite time you could lose serious points. Coherent, readable exposition of your work is half the job in mathematics.

Problem 1 :
Let G be a group and assume that for all $g \in G$ we have $g^{-1} = g$. Prove that G is abelian.

Solution : Let $a, b \in G$, $ab = a^{-1}b^{-1} = (ba)^{-1} = ba$. So that G is abelian.

Problem 2 :
In S_4, consider the subset

$$H = \{I_d, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}\}$$

1. Compute the inverses of the elements H.

2. Is H a subgroup of G. Justify your answer.

Solution :

1. $Id^{-1} = Id$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$.
2. H is not a subgroup of G. Since,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \notin H$$

So H is not closed under multiplication.

Problem 3 : Let $H = \{\sigma \in S_n : \sigma(1) = 1\}$. Prove that H is not a normal subgroup of S_n for $n \geqslant 3$.

Solution : Let $n = 3$, $\tau = (1,2)$ and $\sigma = (2,3)$. Note that $\sigma(1) = 1$ but still,

$$\tau^{-1}\sigma\tau(1) = \tau^{-1}\sigma(2) = \tau^{-1}(3) = 3.$$

Problem 4 :
Let G be the group of all polynomials pf degree n with real coefficients, that is

$$G = \{P(x) : P(x) = a_0 + a_1x + \cdots + a_nx^n, a_i \in \mathbb{R}\}$$

with addition operation defined by : for $P(x) = a_0 + a_1x + \cdots + a_nx^n$ and $Q(x) = b_0 + b_1x + \cdots + b_nx^n \in \mathbb{R}$

$$P(x) + Q(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$$

Let $\phi : (G, +) \to (\mathbb{R}, +)$ be the evaluation homomorphism given by

$$\phi(P(x)) = P(0)$$

1. **Prove that ϕ is homomorphism and that it is surjective but not injective.**
2. **Find the kernel of ϕ.**
3. **Prove that the induced map**

$$\begin{array}{rccc} \bar{\phi}: & (G/Ker(\phi), +) & \to & (\mathbb{R}, +) \\ & [P(x)] & \mapsto & P(0) \end{array}$$

   is a well defined isomorphism.

Solution :

1. Let $P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ and $Q(x) = b_nx^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0$ Then
$$\phi(P(x) + Q(x)) = a_0 + b_0 = \phi(P(x)) + \phi(Q(x))$$
For any $r \in \mathbb{R}$, take $P(x) = r$ then $\phi(P(x)) = r$, So ϕ is surjective. Take $P(x) = 0$ and $P(x) = x$. Then $\phi(P(x)) = \phi(Q(x))$ but $P(x) \neq Q(x)$, so ϕ is not injective.
2. $$\begin{aligned} Ker(\phi) &= \{P(x) \in G | \phi(P(x)) = 0\} \\ &= \{P(x) \in G : P(x) = a_1x + a_2x^2 + \cdots + a_nx^n\} \\ &= \{ \text{ polynomial of any degree } n \text{ with constant coefficient } a_0 \text{ zero}\} \end{aligned}$$
3.(a) Let $P(x)$ and $Q(x)$ be two polynomial such that $[P(x)] = [Q(x)]$ that is $P(x) - Q(x) \in Ker(\phi)$ so that $P(0) - Q(0) = 0$ and $P(0) = Q(0)$. Finally, $P(0) = Q(0)$. And we have proven that $\bar{\phi}$ is a well defined map.

   (b) Let $P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ and $Q(x) = b_nx^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0$ Then
$$\bar{\phi}([P(x)] + [Q(x)]) = a_0 + b_0 = \bar{\phi}([P(x)]) + \bar{\phi}([Q(x)])$$
So $\bar{\phi}$ is a homomorphism.
Similarly as before, for any $r \in \mathbb{R}$, take $P(x) = r$ then $\bar{\phi}(P(x)) = r$. So ϕ is surjective.
For injectivity, let $P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ and $Q(x) = b_nx^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0$. Suppose that $\phi([P(x)]) = \phi([Q(x)])$ that is $a_0 = b_0$ so that $P(x) - Q(x) \in Ker(\bar{\phi})$. That is, $[P(x)] = [Q(x)]$. That proves that $\bar{\phi}$ is injective.

Problem 5 : Let $G = \mathbb{Z}/n\mathbb{Z}$ (n is a fixed integer ; if x is any integer, x is the class of x modulo n).

1. **If $a \in \mathbb{Z}$, prove that $\phi_a : G \to G$ defined by**

$$\phi_a([x]) = [ax]$$

   is a well defined, group homomorphism and depends only on $[a]$. Prove that all homomorphisms $G \to G$ are of this type.

2. **Prove that ϕ_a is an automorphism if and only if there exists b such that $ab \equiv 1(\ mod\ n)$.**

3. **Prove that if n is prime, then $|Aut(\mathbb{Z}/n\mathbb{Z})| = n - 1$.**

Solution :

1. For any $[x] = [y]$ the $[ax] = [a][x] = [a][y] = [ay]$. So that ϕ_a is well defined. Also, $\phi_a([x]) = [ax] = [a].[x]$, so ϕ_a depends only on $[a]$. Finally,

$$\phi_a([x] + [y]) = \phi_a([x + y]) = [a(x + y)] = [a.x] + [a.y] = \phi_a(x) + \phi_a(y)$$

   and ϕ_a is a group homomorphism. If ϕ is any group homomorphism $G \to G$, let $a \in \mathbb{Z}$ be such that $[a] = \phi([1])$. Then $\phi([1]) = \phi_a([1])$, hence $\phi = \phi_a$, since $[1]$ generates the cyclic group G indeed $[k] = k[1]$. Since then necessarily by the property of an homomorphism. We have

$$\phi([k]) = \phi(k \cdot [1]) = k\phi([1])$$

   for all $k \in \{0, \cdots, n\}$.

2. ϕ_a is an automorphism iff there exists an inverse automorphism, which must be of the form ϕ_b for some b. Since we have see that all the automorphism are of this form.
   It is easy to see that $\phi_a \circ \phi_b = \phi_{ab}$, and $\phi_{ab} = Id_G$ iff $ab = 1$, that is $ab \equiv 1(mod n)$.

3. From the previous question,

$$|Aut(\mathbb{Z}/n\mathbb{Z})| = |U_n| = n - 1$$

   since n is prime.