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 :
By using the multiplication table, show that there is only one (up to isomorphism) group of order 3.

$*$	e	a	b
e			
a			
b			

Solution : *Clearly $a * b = e$ since if it's a or b then it follows that $b = e$ or $a = e$ respectively. Likewise, $b * a = e$. We need to determine what $a * a$ and $b * b$ are. $a * a$ can't be a since $a \neq e$. If $a * a = e$ then $a * a = a * b$ and it follows that $a = b$. Therefore $a * a = b$. Likewise, $b * b = a$.*

Problem 2 :

1.(a) **Give the definition of a cyclic group.**

(b) **Give the definition of an commutative group.**

(c) **Show that every cyclic group is commutative.**

2. **Consider the group $\mathbb{Z}/16\mathbb{Z}$ of residues modulo 16 (under addition modulo 16). How many subgroups does this group have ? Explain your answer.**

Solution :

1.(a) A group G is cyclic if there is an $a \in G$ such that

$$G = \{a^n : n \in \mathbb{Z}\}$$

In other words, for any $g \in G$, then there is an integer n (depending on g) such that $g = a^n$. In this case, a is said to generate G or to be a generator of G. A group G is abelian if $gh = hg$, for any $g, h \in G$.

(b) Suppose G is cyclic and that a generates G. Let $g, h \in G$. Thus there are integers k and l such that $g = a^k$ and $h = a^l$. Hence

$$gh = a^k a^l = a^{k+l} = a^{l+k} = a^l a^k = hg$$

and so G is abelian.

2. The group $\mathbb{Z}/16\mathbb{Z}$ is cyclic. From class, a finite cyclic group of order n has a unique subgroup of order d for each (positive) divisor d of n and no other subgroups. Thus number of subgroups of $\mathbb{Z}/16\mathbb{Z}$ is equal to the number of divisors of 16 which is 5.

Problem 3 :
Let

$$G = \{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{Z} \text{ with } a = \pm 1\}$$

1. **Show that G is a group under matrix multiplication.**
2. **Is G abelian ? Explain your answer.**
3. **Describe all elements of order two in G.**

Solution :

1. Let $g = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ and $g' = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$ be elements of G. Then

$$gg' = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad + b \\ 0 & 1 \end{pmatrix}$$

Note $ac = \pm 1$ (since $a = \pm 1$ and $c = \pm 1$) and clearly $ad + b \in \mathbb{Z}$. Thus $gg' \in G$. In other words, matrix multiplication defines a binary operation on G. This is an associative operation (since matrix multiplication for matrices with integer *entries is associative). The usual* 2×2 *identity matrix* $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *is an identity element (since* $AI_2 = A = I_2A$*, for any* 2×2 *matrix* A *with say integer entries). For any* $g = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ *in* G*, the matrix* g *is invertible with inverse* $g^{-1} = \begin{pmatrix} 1/a & -b/a \\ 0 & 1 \end{pmatrix}$ *(Check this!) Since* $a = \pm 1$*, we see that* $1/a = \pm 1$ *and* $-b/a \in \mathbb{Z}$ *and thus the matrix* g^{-1} *belongs to* G*. This proves that* G *is a group under matrix multiplication.*

2. *No,* G *is not abelian. For example,*

$$\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 0 & 0 \end{pmatrix}$$

while

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix}$$

so that

$$\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$$

3. *An element* $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ *in* G *has order two if and only if it not the identity and*

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a^2 & ab+b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

So we must have $a = \pm 1$ *and* $b(a+1) = 0$*. Note* $b \neq 0$ *implies* $a =?1$*. On the other hand,* $b = 0$ *and* $a = 1$ *gives* I_2 *which has order one, not two. Hence* $a =?1$ *for all elements of order two. Thus the elements of order two are exactly the matrices* $\begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix}$ *as* b *varies through* $\mathbb{Z}$*.*

Problem 4 :

1. **State Lagrange's theorem.**
2. **Show that every group of prime order is cyclic.**
3. **The set of ordinary integers Z is a subgroup of the additive group of rational numbers $\mathbb{Q}$. Show that $\mathbb{Z}$ has infinite index in $\mathbb{Q}$ (that is, there are infinitely many (left or right) cosets of $\mathbb{Z}$ in $\mathbb{Q}$).**

Solution :

1. *Let* G *be a finite group and let* H *be a subgroup of* G*. Then the order of* H *divides the order of* G*.*

2. *Suppose $|G|$ is prime. Let $g \in G$ with $g \neq 1$. Then $< g >= \{g^n : n \in \mathbb{Z}\}$ is subgroup of G. By Lagrange ?s Theorem, $| < g > |$ divides $|G|$. Note $| < g > | > 1$ as $g \in < g >$ (and $1 \in < g >$). Since $|G|$ is prime, it follows that $| < g > | = |G|$. Thus $< g >= G$, and G is cyclic.*

3. *Let $x, y \in \mathbb{Q}$ with $0 \leqslant x < 1$ and $0 \leqslant y < 1$. We have $x + \mathbb{Z} = y + \mathbb{Z}$ if and only if $x - y = n$, for some $n \in Z$. Since x and y are each in the interval $[0, 1)$, this is only possible if $x = y$. Thus the cosets $x + \mathbb{Z}$, for $0 \leqslant x < 1$, form an infinite family of distinct cosets of $\mathbb{Z}$ in $\mathbb{Q}$. (In fact, these are all the cosets of $\mathbb{Z}$ in $\mathbb{Q}$.)*

Problem 5 :

Let G be a finite group, X be a set and $G \times X \to X$ be a group action. Let $x_0 \in X$.

1. **Give the definition of the stabilizer $Stab(x_0)$ of x_0.**
2. **Give the definition of the orbit $O(x_0)$ of x_0.**
3. **Prove that**

$$\psi : G/Stab(x_0) \to O(x_0) \qquad \textbf{where} \qquad \psi(g \cdot Stab(x_0)) = g \cdot x_0 \tag{1}$$

   is a well define map.
4. **Prove that ψ is a bijection.**
5. **Deduce that the size $|O_{x_0}|$ of any individual orbit must divide $|G|$.**

Solution : *Let $H = \mathrm{Stab}_G(x_0)$. There is a bijective correspondence between $G/H = \{xH : x \in G\}$ and points in X, implemented by the map*

$$\psi : G/H \to X \qquad \textit{where} \qquad \psi(gH) = g \cdot x_0 \tag{2}$$

This map is well-defined – i.e. if we take a different coset representative g' such that $g'H = gH$, we still get $\psi(g'H) = \psi(gH)$. [We have $g'H = gH \Leftrightarrow$ there is some $h \in H$ such that $g' = gh$, but then

$$g' \cdot x_0 = (gh) \cdot x_0 = g \cdot (h \cdot x_0) = g \cdot x_0 \quad ,$$

since $h \cdot x_0 = x_0$ by definition of the stabilizer $H = \mathrm{Stab}_G(x_0)$.] Furthermore ψ is an onto map because the action is transitive. [Given $y \in X$ there is some $g \in G$ such that $y = g \cdot x_0$, and then $\psi(gH) = g \cdot x_0 = y$.] Finally, ψ is a one-to-one map (so $\psi : G/H \to X$ is a bijection). In fact, if $\psi(g_1H) = \psi(g_2H)$ we have $g_1 \cdot x_0 = g_2 \cdot x_0$, which implies that $g_1^{-1} \cdot (g_2 \cdot x_0) = (g_1^{-1}g_2) \cdot x_0 = x_0$. Since $g_1^{-1}g_2$ fixes x_0 it is in $\mathrm{Stab}_G(x_0) = H$; thus $g_1^{-1}g_2 = h \in H$, and $g_2H = (g_1h)H = g_1H$ as required. Since ψ is a bijection we must have $|X| = |G/H|$. We finish the proof by applying Lagrange's theorem, which says that $|G| = |G/H| \cdot |H|$ for any subgroup.