Midterm 1 / 2009.3.5 / MAT 4233.001 / Modern abstract algebra

Note Title 3/5/2009

1. Prove that $a \in \mathbf{Z}_n$ has a multiplicative inverse if and only if a is relatively prime to n. What is the multiplicative inverse of 3 in $\mathbf{Z}_{10}$?

Let $a \in \mathbb{Z}_n$. Let $d = \gcd(a,n)$.

$\Rightarrow$ Suppose $\exists\, a' \in \mathbb{Z}_n$ with $aa' \equiv 1 \bmod n$

Then $n \mid aa'-1$ so $d \mid aa'-1$

But $d \mid a$ so $d \mid aa'$ so $d \mid 1$ so $d = 1$ ☺

$aa'-(1-aa')$

$\Leftarrow$ Bezout $\Rightarrow d = sa + tn$ for some $s,t \in \mathbb{Z}$

If $d = 1$ $1 = sa + tn$ so $n \mid 1 - sa$

so $sa \equiv 1 \bmod n$ ☺

$3^2 = 9$, $3^3 = 27 = 7$, $3^4 = 21 = 1$ $\therefore$ $3^{-1} = 3^3 = \boxed{7}$

2. Suppose G is a group where each nontrivial element has order 2. Prove that G is abelian.

$\forall x \in G$ $x^2 = e$, so $x = x^{-1}$

Let $a, b \in G$. Then $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ ☺

3. Suppose G is a cyclic group of order 18. How many subgroups does it have? Explain.

There is exactly one subgroup for each divisor d of 18 generated by $a^{18/d}$

$d = 1$: $\langle a^{18} \rangle = \langle e \rangle$	6 : $\langle a^3 \rangle$		
2 : $\langle a^9 \rangle$	9 : $\langle a^2 \rangle$		total: $\boxed{6}$
3 : $\langle a^6 \rangle$	18 : $\langle a \rangle = G$		

4. Suppose G is a group with $|G|$ a power of 2. Prove that G has an element of order 2.

Suppose $|G| = 2^n$ for some $n \in \mathbb{Z}^+$

Let $a \in G$, $a \neq e$.

Lagrange $\Rightarrow$ $|a| = |\langle a \rangle|$ divides $|G| = 2^n$

so $|a| = 2^k$ for some $k \in \mathbb{Z}^+$

Let $x = a^{2^{k-1}}$. Then $x \neq e$

But $x^2 = \left(a^{2^{k-1}}\right)^2 = a^{2^{k-1} \cdot 2} = a^{2^k} = e$ ☺

5. Let $H = \{(), (12)(34), (13)(24), (14)(23)\}$. Prove that H is a subgroup of S_4 (you may use the word *similarly* as appropriate). What is its index? Is H isomorphic to $\mathbf{Z}_4$? Explain.

* identity: $() \in H$ ☺
* closure: $(12)(34)(12)(34) = () \in H$

  $(12)(34)(13)(24) = (14)(23) \in H$

  others are similar ☺
* inverses: $(12)(34)(12)(34) = ()$

  others are similar ☺

  } Note: Since H is finite this is automatic! ☺

Lagrange $\Rightarrow$ $|S_4| = |H| \cdot \text{index}$, where $|S_4| = 4!$ and $|H| = 4$

$\therefore$ index $= \frac{4!}{4} = 3! = \boxed{6}$

$\boxed{H \not\cong \mathbb{Z}_4}$ because each nontrivial element of H has order 2

But $\mathbb{Z}_4$ has 2 elements of order 4 namely 1 and 3.