Solution for Homework 3 part 1, problem 1 to 5

Recording and typing by 9622534, Bin Yeh

March 23, 2009

1. *Show that a group of order pq has at most one subgroup of order p; where $p > q$ are primes.*

   We will use the fact that if H is a group with $|H| = p$(where p is prime), then H is cyclic.
   Assume there are two subgroups H_1, H_2 with $|H_1| = |H_2| = p$,
   $H_1 \cap H_2 = \{e\}$. Then by fact above we have $H_1 =< a >$ and $H_2 =< b >$ for some a, $b \in G$. Now consider $< a, b >$. Since $< a, b >< G$ we have
   $p < | < a, b > | \leq pq < p^2$. Note that
   $G \supseteq < a, b > \supseteq \{a^i b^j | 0 \leq i, j \leq p-1\}$ and if $a^i b^j$ are all distinct for all $0 \leq i, j \leq p-1$, then $| < a, b > | \geq p^2 > pq = |G|$, a contradiction. Thus we may assume $a^i b^j = a^{i'} b^{j'}$ for some $(i, j) \neq (i', j')$. We have 3 cases.
   (i) $i = i'$ and $j \neq j'$
   Then we have $b^j = b^{j'}$, a contradiction.
   (ii) $i \neq i'$ and $j = j'$
   Similar to case (i).
   (iii) $i \neq i'$ and $j \neq j'$
   Then $a^{i-i'} = b^{j-j'}$. Since $H_1 \cap H_2 = \{e\}$ we have $a^{i-i'} = b^{j-j'} = e$, therefore $i = i'$ and $j = j'$, a contradiction. Thus we are done. ■

   Comment from teacher: It's easier to prove it by using
   $pg = |G| \geq |H_1 H_2| = \frac{|H_1||H_2|}{|H_1|\cap|H_2|} = p^2$, a contradiction.

2. *Let G be the group of all nonzero complex numbers under multiplication and let N be the set of complex numbers of absolute value 1. Show that $G = N$ is isomorphic to the group of all positive real numbers under multiplication.*

   Let $f : G \mapsto \mathbb{R}^+$ by $f(x) = |x|$. It's routine to check f is well-defined, onto, homomorphism and $ker(f) = N$. Then by first homomorphism theorem we have $G/N \cong \mathbb{R}^+$. ■

3. *Let G be the group of real numbers under addition and let N be the subgroup of G consisting of all the integers. Prove that G/N is isomorphic to the group of all complex numbers of absolute value 1 under multiplication.*

   Let $\alpha : G/N \mapsto U = \{z | z \in \mathbb{C}, |z| = 1\}$ by
   $\alpha(r + \mathbb{Z}) = cos(2\pi r) + isin(2\pi r) = e^{i2\pi r}$.
   To show α is well-defined and 1-1, we have
   $r + z = s + z$
   $\iff r - s = n, n \in \mathbb{Z}$

$\iff e^{i2\pi(r-s)} = e^{i2\pi n} = 1$
$\iff e^{i2\pi r}e^{i2\pi(-s)} = 1$
$\iff e^{i2\pi r} = e^{i2\pi s}$
To show α is onto, for all $e^{i\theta} \in U$, there exists $r = \frac{\theta}{2\pi} \in \mathbb{R}$ such that
$\alpha(r + \mathbb{Z}) = \alpha(\frac{\theta}{2\pi} + \mathbb{Z}) = e^{i2\pi\frac{\theta}{2\pi}} = e^{i\theta}$
For homomorphism,
$\alpha(r+\mathbb{Z}+s+\mathbb{Z}) = \alpha(r+s+\mathbb{Z}) = e^{i2\pi(r+s)} = e^{i2\pi r}e^{i2\pi s} = \alpha(r+\mathbb{Z})\alpha(s+\mathbb{Z})$
Thus α is isomorphic. ■

Comment from teacher:
Let $\phi : \mathbb{R} \mapsto U$ by $\phi(r) = e^{2\pi ri}$. Then by first homomorphism theorem we have $U \cong \mathbb{R}/ker(\phi)$.

4. *Prove that every finite group having more than two elements has a nontrivial automorphism.*

We consider 2 cases separately.
(i) G is non-abelian
Then fix $a \in G$, $a \neq e$, $a \notin C(G)$. Let $f : G \mapsto G$ by $f(x) = axa^{-1}$.
It's easy to show f is homomorphism since
$f(xy) = axya^{-1} = axa^{-1}aya^{-1} = f(x)f(y)$.
For 1-1, if $f(x) = f(y) \Rightarrow axa^{-1} = aya^{-1} \Rightarrow x = y$.
Since f is 1-1 and G is finite, f is onto.
It reminds to show that f is non-trivial, i.e. f is not identity. Suppose f is identity, then $axa^{-1} = x$ for all $x \in G$. Thus $ax = xa$ for all $x \in G$, contradicts that a is not in the center of G.
(ii) G is abelian
We have 2 cases here.
(1) $\exists x \in G$ with $x \neq x^{-1}$
Then let $f(x) = x^{-1}$. It's non-trivial from the assumption and easy to check homomorphism, 1-1 and onto.
(2) $x = x^{-1} \forall x \in G$
Claim: $G \cong \mathbb{Z}_2 \bigoplus \mathbb{Z}_2 \bigoplus ... \bigoplus \mathbb{Z}_2 (n \text{ times})$ for some $2 \leq n$
Claim shall be proved later. Let e_i be all zero except at the ith position, it's 1. Then let f(x) be

$$f(x) = \begin{cases} e_2, & \text{if } x = e_1 \\ e_1, & \text{if } x = e_1 \\ x, & \text{otherwise.} \end{cases}$$

It's clearly non-trivial. Rest are routine to do.(check homomorphism, 1-1 and onto)
To prove the claim, let $U = \{a_1, ..., a_n\}$ be a set with $< U >= G$ with no proper subset of U generates G. It can be showed that
$G \cong < a_1 > \bigoplus \cdots \bigoplus < a_n >$ by let $\phi : G \mapsto < a_1 > \bigoplus \cdots \bigoplus < a_n >$ by for $x = a_1^{m_1} a_2^{m_2} ... a_n^{m_n}$, $\phi(x) = (a_1^{m_1}, a_2^{m2}, ..., a_n^{m_n})$
Again ϕ can be checked as well-defined, 1-1, onto thus ϕ is an isomorphism.

Since $x = x^{-1}$ $\forall x \in G$, $< a_i > \cong \mathbb{Z}_2$ $\forall i$. Since $|G| > 2$, $n \geq 2$. Therefore claim is proved. ■

Comment from teacher:
One may try the following function for the last case:

$$f(x) = \begin{cases} b, & \text{if } x = a \\ a, & \text{if } x = b \\ x, & \text{otherwise.} \end{cases}$$

where $a \neq b$ and $a \neq e, b \neq e$.

5. *Prove that any element $\sigma \in S_n$ which commutes with $(1, 2, ..., r)$ is of the form $\sigma = (1, 2, ..., r)^i \tau$ for some $\tau \in S_n$ with $\tau(i) = i$ for all $1 \leq i \leq r$.*

($\Leftarrow$)
Easy to check by some routine works.

($\Rightarrow$)
$\sigma(1, ..., r) = (1, ..., r)\sigma \Rightarrow \sigma(1, ..., r)\sigma^{-1} = (1, ..., r)$
$\Rightarrow (\sigma(1), ..., \sigma(r)) = (1, ..., r)$ (This is a result from lecture note)
$\therefore$ if $\sigma(1) = j$, then $\sigma(2) = j + 1$, ..., $\sigma(j) = j + r - 1(\text{mod } r)$
Thus it must be in the form as showed in the problem. ■