MAT1100

Algebra I

Assignment 2

Contents

Tyler Holden - Fall 2011

1. Problem 1

1.1. Part a. What is the least integer n for which the symmetric group S_n contains an element of order 18.

We recall that if an element σ has cycle structure $[n_1, n_2, \ldots, n_k]$ then $|\sigma| = \text{lcm}(n_1, n_2, \ldots, n_k)$. Thus to find the smallest S_m such that $\sigma \in S_m$ and $|\sigma| = 18$ we need $\text{lcm}(n_1, \ldots, n_k) = 18$ and $\sum n_i = m$.

We first note that the order of every element must divide the order of the group. Consequently, if σ has order 18 it cannot be S_n for $n < 6$. By brute force checking, one can see that that the smallest group in which the desired σ exists is S_{11} in which any element with cycle structure $[9, 2]$ has order 18.

Indeed, I have verified this by executing the following Matlab commands, the source code for which is located at the end of this treatise.

```
>>grpSize = smallestSymGrp(18);
grpSize =
    11
```

1.2. Part b. What is the maximal order of an element in S_{26}?

As we noted in part a, the order of the largest element in S_{26} will be given by the least common multiple of all possible partitions of 26. We note that there are 2436 partitions of 26. While there may be a clever way of determining the result, I have again used code to determine the maximal order. It is executed as follows:

```
>>max(compSymOrders(26);
ans =
        1260
```

So the maximal order of an element in S_{26} is 1260 and this corresponds to an element with cycle structure [1 4 5 7 9].

2. Problem 2

Let H be a subgroup of index 2 in a group G. Show that $H \triangleleft G$.

Note that since $[G : H] = 2$ then H partitions G into two cosets. Let $\pi : G \to G/H$ where G/H is the set of cosets. We explicitly state at this point that we are <u>not</u> assuming that π is a group homomorphism. However, as a set map we define $h \in H$ then $\pi(h) = H$ and if $g \notin H$ then $\pi(g) = gH \neq H$.

Claim 1. *If $g, g' \notin H$ then $gg' \in H$.*

Proof. For the sake of contradiction, assume that $gg' \notin H$. Then $\pi(gg') = gg'H \neq H$. But since $g \notin H$ then $\pi(g) = gH \neq H$. Since there are only two elements of G/H we must have that $gH = gg'H$. But then $g'H = H$ which is a contradiction, since we also assumed that $g' \notin H$. □

Claim 1 actually indicates to us that G/H has a group structure, since the multiplication table of G/H satisfies that of C_2. However, to be more rigorous, it is now relatively simple to show that $H \triangleleft G$. Let $g \in G$, and consider the following two cases:

Case 1 ($g \in H$): If $g \in H$ then $gHg^{-1} = H$ trivially, and so H is preserved under conjugation by g.

Case 2 ($g \notin H$): Assume that $g \notin H$. Let $h \in H$ be an arbitrary element, and consider ghg^{-1}. Now $gh \notin H$ since otherwise $gH = H$ but this cannot be the case. But then ghg^{-1} is the product of two elements which are not in H, and by Claim 1 it follows that $ghg^{-1} \in H$ as desired.

Both Case 1 and Case 2 above imply that for every element $g \in G$ we have that $gHg^{-1} = H$ and so $H \triangleleft G$ as required.

3. Problem 3

Let $\sigma \in S_{20}$ be a permutation whose cycle decomposition is $[5, 3, 3, 2, 1, 1, 1, 1, 1, 1, 1]$. What is the order of the centralizer $C_{S_{20}}(\sigma)$?

Consider the group action of S_{20} on itself via conjugation and recall from Lagrange's Theorem that $|G| = [G : C_G(\sigma)]|C_G(\sigma)|$. Hence the order of the centralizer of σ will be $|G|$ divided by the index of $C_G(\sigma)$ in G. However, by the Orbit - Stabilizer Theorem, we know then that $[G : C_G(\sigma)]$ is the order of the orbit of σ under the group action, and so is the number of conjugacy classes of σ.

Using a combinatoric counting argument, we then know that the number of conjugacy classes of an element with cycle type $[5, 3, 3, 2, 1, 1, 1, 1, 1, 1, 1]$ is going to be

$$[G : C_G(\sigma)] = \frac{20!}{(5^1 \cdot 1!)(3^2 \cdot 2!)(2^1 \cdot 1!)(1^7 \cdot 7!)} = \frac{20!}{4 \cdot 5 \cdot 9 \cdot 7!}$$

Thus

$$|C_G(\sigma)| = \frac{|G|}{[G : C_G(\sigma)]} = 4 \cdot 5 \cdot 9 \cdot 7! = 907200$$

4. Problem 4

Let G be a group of odd order. Show that x is not conjugate to x^{-1} unless $x = e$.

We note that since G has odd order and the order of every element of G must divide $|G|$ then every element of G must also have odd order. Now assume that $\exists g \in G$ such that $gxg^{-1} = x^{-1}$. By applying the inverse to both sides of this equation we find that $x = gx^{-1}g^{-1}$. Substituting our original equation into this yields $x = g(gxg^{-1})g^{-1} = g^2xg^{-2}$

Claim 2. *If n is even then $x = g^n x g^{-n}$. If n is odd, then $x = g^n x^{-1} g^{-n}$.*

Proof. We shall proceed by induction. We note that the base case of $n = 1$ and $n = 2$ have already been shown. Thus assume that n is even so that $x = g^n x g^{-n}$. Substituting $x = gx^{-1}g^{-1}$ we get

$$x = g^n(gx^{-1}g^{-1})g^{-n} = g^{n+1}x^{-1}g^{-(n+1)}$$

and $n + 1$ is odd so this shows the required result for n odd. On the other hand, assume that n is odd, so that $x = g^n x^{-1} g^{-n}$. Substituting $x^{-1} = gxg^{-1}$ we get

$$x = g^n(gxg^{-1})g^{-n} = g^{n+1}xg^{-(n+1)}$$

and $n + 1$ is even, so this shows the result for n even. □

Now since $|G|$ is odd, then $|g|$ is odd, and so $x = g^{|g|}x^{-1}g^{-|g|} = x^{|g|}x^{-1}\left(x^{|g|}\right)^{-1} = x^{-1}$.

Claim 3. *If $|G|$ is odd, then the only element in G for which $x = x^{-1}$ is e.*

Proof. If $x = x^{-1}$ then $x^2 = e$. But by a Lemma (which I proved in assignment one) this implies that $|x| \,\Big|\, 2$. Since the order of $|G|$ is odd, no element can have even order, so $|x| = 1$ and we conclude that $x = e$. □

Hence we have shown that in a group of odd order, the only element which can be conjugate to its own inverse is the identity element.

5. Problem 5

So that if $G/Z(G)$ is cyclic then G is abelian.

We already know that $Z(G) \triangleleft G$ and so $G/Z(G)$ is a group. Assume further that $G/Z(G)$ is cyclic, and fix a generator $xZ(G)$ so that $\langle xZ(G)\rangle = G/Z(G)$. Let g, h be arbitrary elements of G and consider their projections onto the quotient group by $\pi : G \to G/Z(G)$ as $\bar{g} = \pi(g)$ and $\bar{h} = \pi(h)$. But since $G/Z(G)$ is cyclic, $\exists n, m \in \mathbb{N}$ (possibly the same) such that $\bar{g} = (xZ(G))^n = x^n Z(G)$ and $\bar{h} = (xZ(G))^m = x^m Z(G)$. By definition of the projection map, it then follows that $\exists z_g, z_h \in Z(G)$ such that $g = x^n z_g$ and $h = x^m z_h$. Then z_g and z_h commute with all elements of G so

$$\begin{aligned} gh &= (x^n z_g)(x^m z_h) = (z_h x^n)(x^m z_g) && \text{since } z_g, z_h \text{ commute with everything} \\ &= z_g x^{n+m} z_h = z_g (x^m)(x^n) z_h \\ &= (x^m z_h)(x^n z_g) && \text{again since } z_g, z_h \in Z(G) \\ &= hg \end{aligned}$$

Since g, h were arbitrary, this must hold for all g, h and so G is abelian.

6. Problem 6

Prove that if the group of automorphisms of a group G is cyclic then G is abelian.

Note that this is actually a more powerful hypothesis than necessary. Indeed, assume that $\mathrm{Aut}(G)$ is cyclic. Since every subgroup of a cyclic group is cyclic and $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$ then $\mathrm{Inn}(G)$ is also cyclic.

Claim 4. $G/Z(G) \cong \mathrm{Inn}(G)$.

Proof. For every $g \in G$ denote by ϕ_g the inner automorphism $\phi_g(h) = ghg^{-1}$. Define the map $\Phi : G \to \mathrm{Inn}(G)$ by $\Phi(g) = \phi_g$.

To show that Φ is a homomorphism, we first note that

$$\phi_g \circ \phi_h(x) = \phi_g(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \phi_{gh}(x).$$

so that $\phi_g \circ \phi_h = \phi_{gh}$. Similarly, note that

$$\phi_g \circ \phi_{g^{-1}}(x) = \phi_{gg^{-1}}(x) = \phi_e(x) = x$$

so $(\phi_g)^{-1} = \phi_{g^{-1}}$. But then $\Phi(gh) = \phi_{gh} = \phi_g \circ \phi_h = \Phi(g) \circ \Phi(h)$, implying that Φ perserves the group products; and $\Phi(g^{-1}) = \phi_{g^{-1}} = (\phi_g)^{-1} = \Phi(g)^{-1}$ so Φ preserves inverses. Hence Φ is a homomorphism.

Now clearly Φ is surjective since every inner-automorphism is, by definition, of the form ϕ_g. Finally, we wish to characterize the kernel of Φ. Note that if $g \in \ker \Phi$ then $\Phi(g) = \phi_e$. But $\Phi(g) = \phi_g$ so if $h \in G$ is arbitrary, then $\phi_g(h) = ghg^{-1} = \phi_e(h) = h$ so $gh = hg$. Since h was arbitrary, this must hold for all h so $g \in Z(G)$ and $\ker \phi \subseteq Z(G)$. Conversely, if $g \in Z(G)$ then $ghg^{-1} = h$ so $\phi_g(h) = h$ for every h. Hence $\phi_g = \phi_e$ implying that $Z(G) \subseteq \ker \Phi$. Both inclusions imply that $Z(G) = \ker \Phi$ so by the first isomorphism theorem

$$G/Z(G) \cong \mathrm{Inn}(G)$$

as required. □

But we noted that $\mathrm{Aut}(G)$ cyclic implies that $\mathrm{Inn}(G)$ is cyclic implies that $G/Z(G)$ is cyclic. By Problem 5, it follows that G is abelian as required.

7. Problem 7

7.1. **Part a. Let G be a group and $H \leq G$ such that $[G : H] < \infty$. Prove that $\exists N \triangleleft G$ such that $N \subseteq H$ and $[G : N] < \infty$.**

We first note the following:

Claim 5. *There is a bijective correspondence between the set of left-group actions of a group G on a set X, and the set of group homomorphisms $\sigma : G \to S_X$.*

Proof. Let ρ be our left group action, and define $\sigma : G \to S_X$ by $\sigma(g)(x) = \rho(g, x)$. Now

$$\begin{aligned}\sigma(gh)(x) = \rho(gh, x) = \rho(g, \rho(h, x)) = \sigma(g)\rho(h, a) = \sigma(g)(\sigma(h)(x))\\ = \sigma(g) \circ \sigma(h)(x)\end{aligned}$$

so σ preserves the product. On the other hand

$$\sigma(g^{-1}) \circ \sigma(g)(x) = \sigma(g^{-1}g)(x) = \sigma(e_G)(x) = \rho(e_G)(x) = x$$

so σ also preserves inverses.

Conversely, if $\sigma : G \to S_X$ is a group homomorphism, define $\rho : G \times X \to X$ as $\rho(g, x) = \sigma(g)(x)$. The exact same argument as above (only done in the opposite direction) tells us that ρ is indeed a group action. □

Let $n = [G : H]$ which is finite by assumption. Consider the left-action of G on the *set* G/H by left-multiplication. Since $|G/H| = [G : H] = n$ then $S_{G/H} \cong S_n$ so let $\phi : G \to S_n$ be the corresponding homomorphism, guaranteed to exist and defined by Claim 5. However, for the sake of clarity, we will continue to associate elements of S_n with the equivalence classes of G/H.

Claim 6. $\ker \sigma \subseteq H$.

Proof. Let $g \in \ker \phi$ and notice then that $\phi(g)(sH) = sH$ since the image of elements in the kernel is just the identity map. However, $\phi(g)(sH) = \rho(g, sH) = gsH$ for every $sH \in S_n$. Thus $gsH = sH$ so in particular this must hold for the identity in G/H, implying that $gH = H$. However, this is only true if $g \in H$, so $\ker \phi \subseteq H$ as required. □

Hence $\ker \phi \lhd G$ and $H \supseteq \ker \phi$. All that remains to be shown is that $[G : \ker \phi]$ is finite. However, by the first isomorphism theorem $G/\ker \phi \cong \operatorname{im} \phi$ which is a subgroup of S_n. This means that $|\operatorname{im} \phi| \,\Big|\, p!$ and so $[G : \ker \phi] = |\operatorname{im} \phi| \,\Big|\, p!$ so $[G : \ker \phi]$ is finite as required.

7.2. **Part b. Let G be a group and H_1 and H_2 be subgroups such that $[G : H_1] < \infty, [G : H_2] < \infty$. Show that $[G : H_1 \cap H_2] < \infty$.**

Since $[G : H_1], [G : H_2]$ are both finite, we note that it is sufficient to show that $[G : H_1 \cap H_2] \leq [G : H_1][G : H_2]$ from which the result will follow. We first recall that if $H_1, H_2 \leq G$ then $H_1 \cap H_2 \leq G$. Then

Claim 7. *If $H_1, H_2 \leq G$ are disjoint subgroups of G, then for every coset xH_1 and yH_2 their intersection $xH_1 \cap yH_2$ is either empty or a coset of $H_1 \cap H_2$.*

Proof. Fix two cosets xH_1 and yH_2. If $xH_1 \cap yH_2 = \emptyset$ we are done. Thus assume that $xH_1 \cap yH_2 \neq \emptyset$ and choose g in this set. By definition, $g \in xH_1$ and xH_2, so $\exists h_1 \in H_1, h_2 \in H_2$ such that $g = xh_1$ and $g = xh_2$. But then

$$gH_1 = xh_2H_1 = xH_1, \qquad gH_2 = yh_2H_2 = yH_2$$

and so $g(H_1 \cap H_2) = gH_1 \cap gH_2 = xH_1 \cap yH_2$, so $xH_1 \cap yH_2$ is a coset of $H_1 \cap H_2$. □

[6] It is then easy to see a (possibly poor) upper bound on the number of cosets of $H_1 \cap H_2$ will be given by the total number of possible intersections of cosets of H_1 and H_2. That is, if every coset of H_1 intersects a coset of H_2 non-trivially, then there are at most $[G : H_1][G : H_2]$ cosets of $H_1 \cap H_2$. Hence $[G : H_1 \cap H_2] \leq [G : H_1][G : H_2]$. Since $[G : H_1], [G : H_2] < \infty$ then $[G : H_1 \cap H_2] < \infty$ which is what we wanted to show.

8. Source Code

The following is the source code used for my questions above. Note that these files can be found on my user page on the wiki. On that page I have also included a copy of the m-file `partitions.m` which is a canned algorithm for determining the partitions of a positive integer.

```
function orders = compSymOrders(grpSize)

myParts = partitions(grpSize);
orders = zeros(size(myParts,1),1);

for itrow = 1:size(myParts,1)
    cycle=[];
    for itcol = 1:size(myParts,2)
        cycle = [cycle itcol*ones(1,myParts(itrow,itcol))];
    end
    orders(itrow) = genLCM(cycle);
end

function mylcm = genLCM(array)

if length(array)<2
    mylcm = array;
    return;
elseif length(array)==2
    mylcm = lcm(array(1),array(2));
    return;
else
    mylcm = lcm(array(1),genLCM(array(2:end)));
    return;
end

function grpSize = smallestSymGrp(order)

answerFound=false;
grpSize = 2;
while ~answerFound && grpSize < 100
    orders = compSymOrders(grpSize);
    if ~isempty(find(orders==order, 1))
```

```
        return;
    else
        grpSize = grpSize + 1;
    end
end %end while
```