Math113Hw3

Trustin Nguyen

May 10, 2023

Homework 3

Exercise 1: Show that any group of order 10 is either cyclic or dihedral.

Proof. Let $|G| = 10$. by Lagrange, all elements of G have order 1, 2, 5, or 10. If an element a has order 10, then $\langle a \rangle = G = C_{10}$. if there are no order 5 elements, then it has only order 2 elments, so $|G| = 2^n$ which is not true. So G has an order 5 element, r and order 2 s. Since $\langle r \rangle$ has index 2, $\langle r \rangle \triangleleft G$.
There is $srs^{-1} \in \langle r \rangle$ so there are 5 cases:

1. $srs^{-1} = e$ implies that $sr = s$ which means $r = e$ which is false.
2. $srs^{-1} = r$ implies that $sr = rs$ so sr has order 10, which is not possible since that case was already covered.
3. $srs^{-1} = r^2$ implies that $r = sr^2s^{-1}$.

$$\begin{aligned} srs^{-1}srs^{-1} = sr^2s^{-1} &= r^4 \\ r &= r^4 \\ e &= r^3 \end{aligned}$$

   which is not true.
4. $srs^{-1} = r^3$ implies that $r = sr^3s^{-1}$

$$\begin{aligned} srs^{-1}srs^{-1}srs^{-1} = sr^3s^{-1} &= r^9 \\ r &= r^9 \\ e &= r^8 \end{aligned}$$

   which is not true
5. It must be that $srs^{-1} = r^4 = r^{-1}$, so the group is dihedral.

□

Exercise 2: Let H be a subgroup of finite group G and let K be a subgroup of H. Show that

$$|G : K| = |G : H||H : K|$$

Proof. By Lagrange,

$$\begin{aligned} |H||G : H| &= |G| \\ |K||H : K| &= |K| \end{aligned}$$

So we have

$$\begin{aligned} |G| &= |G : H||H : K||K| \\ \frac{|G|}{|K|} &= |G : H||H : K| \end{aligned}$$

Since the elements of K form a left coset of K, they form an equaivalence class. Since the left cosets partition G and are of the smae size, there are $\frac{|G|}{|K|}$ left cosets. □

Exercise 3: Let G be a finite group and let p be the least prime number dividing the order of G. Let H be a subgroup of index p. By considering the homomorphism

$$G \mapsto S_p$$

given by permuting the set of cosets

$$g \mapsto (aH \mapsto gaH)$$

and the previous exercises, or otherwise, show that H is normal in G.

Proof. consider the kernel of the permutation of the group action

$$\varphi(g) \mapsto (aH \mapsto gaH)$$

with $\ker(\varphi) \leq H$. How with the previous problem,

$$|G : \ker(\varphi)| = |G : H||H : \ker\varphi||G : \ker(\varphi)| = p|H : \ker\varphi|$$

and that $|G : \ker(\varphi)| \leq p!$ by the isomorphism theorem.

$$|H : \ker(\varphi)| \mid (p-1)!$$

then $(p-1)!$ divides the order of G but if $|H : \ker(\varphi)| \neq 1$, that implies that a smaller prime than p dividing $|H : \ker(\varphi)|$ and therefore G. So

$$|H : \ker(\varphi)| = 1$$

and H is the kernel of the group action, making it normal in G. □

Proof Idea: The idea is that we do not know what the kernel of the group homomorphism will look like. The kernel if it was normal would be the entire group, but when we multiply the group K by an element in the coset, if left coset is not equal to right coset, then we do not get the same coset, or the o coset. So the permutation might not land us back in K. So we know that the kernel is a subset of K. But since we make $|G : K|$ minimal, we find that $|G : \ker\varphi|$ is maximized so that the size of the kernel matches that of K.

Exercise 4: Let p, q be not necessarily distinct primes. Show that no group of order pq is simple.

Proof. The group $|G| = pq$ has either elements of order $1, p, q$, or pq. Considering p, q with $p \leq q$. Since p is the least prime number dividing the order of the group, by the last problem, the cyclic group with index p is normal. So no group of order pq is simple. □

Exercise 5: Consider a pack of $2n$ cards, numbered from 0 to $2n-1$. We consider a shuffle where wew split the cards into two equal halves and then interleave the cards such that the top and bottom cards reamin at the top and the bottom, respectively. By expresssing our shuffle as an element of S_{2n}, or otherwise, show that its order (i.e. the smallest number of times we need to shuffle to get back the cards into the original position) is the multiplicative order of 2 modulo $2n-1$, i.e. the least positive k such that $2^k \cong 1 \pmod{2n-1}$. Deduce that after at most $2n-2$ shuffles we get the cards into the original position. What is the order for 52 cards?

Proof. Observe that our shuffle looks something like

$$\begin{aligned} 0 &\mapsto 0 \\ 1 &\mapsto 2 \\ 2 &\mapsto 4 \\ &\vdots \\ n-1 &\mapsto 2n-2 \\ n &\mapsto 1 \\ n+1 &\mapsto 3 \\ &\vdots \\ 2n-1 &\mapsto 2n-1 \end{aligned}$$

We obserce that for $n+1$ and higher, the pattern of doubling continues, but we take the remainder $\mod 2n-1$. So we end up with the bijection

$$f(x) = 2x \mod 2n-1$$

If we look at the orbit of one element, we can consider the number of compositions of the function that it takes for that element to map back to itself. Taking the 1st cord, we see that

$$\begin{aligned} f^k(x) = x \to 2^k(x) &\mod 2n-1 = x \\ 2^k(1) &\mod 2n-1 = 1 \\ 2^k &\mod 2n-1 = 1 \end{aligned}$$

So the order of the group action by $f(x)$ on the set of cards is the smallest k such that $2^k \mod 2n-1 = 1$. We also conclude that it will take at most $2n-2$ shuffles because using the Euler totient function,

$$U_n = \{[x] : \gcd(x, n) = 1\}$$

we notice that it has at most $n-1$ elements whenever $n > 1$, and that for $\varphi(n) = |U_n|$,

$$a^{\varphi(n)} \cong 1 \pmod{n}$$

whenever a and n are relatively prime. So $k \leq 2n-1-1 = 2n-2$. the order for 52 cards is the least k for

$$2^k \cong 1 \pmod{103}$$

Observe that 103 is prime, so we have

$$2^{102} \cong 1 \pmod{103}$$

Now check for all factors of 102: 1, 2, 3, 17, 51, 102:

$$
\begin{aligned}
2^1 &\not\equiv 1 \pmod{103} \\
2^2 &\not\equiv 1 \pmod{103} \\
2^3 &\not\equiv 1 \pmod{103} \\
2^{17} &\equiv (2^7)^2 2^3 \\
&\equiv 25^2 2^3 \\
&\equiv 7(2^3) \\
&\not\equiv 1 \pmod{103} \\
2^{51} &\equiv (2^{17})^3 \\
&\not\equiv 1 \pmod{103} \\
&\equiv (7(2^3))^3 \\
&\equiv (7^3)(2^9) \\
&\equiv (34)(25)(2^2) \\
&\equiv (3400) \\
&\equiv 1 \pmod{103}
\end{aligned}
$$

So the number of shuffles needed is 51. □