Abstract Algebra

Week 3 HW

shaozewxy

August 2022

1

(1.7.11)

Write out the cycle decomposition of the eight permutation in S_4 corresponding to the elements of D_8 given by the action of D_8 on the vertices of a square.

1: 1

r: (1 2 3 4)

r^2: (1 3)(2 4)

r^3: (1 4 3 2)

s: (2 4)

sr: (1 2)(3 4)

sr^2: (1 3)

sr^3: (1 4)(2 3)

2

(1.7.17)

Let G be a group and let G act on itself by left conjugation, so each $g \in G$ map G to G by

$$x \mapsto gxg^{-1}$$

For fixed $g \in G$, prove that conjugation by g is an isomorphism from G onto itself. Deduce that x and gxg^{-1} have the same order for all x in G and that for any subset A of $G, |A| = |gAg^{-1}|$.

Fixing $g \in G$, define $\phi_g : G \to G$ by

$$\phi_g(x) = gxg^{-1}$$

First NTS ϕ_g is injective:

$\forall x, y \in G, \phi_g(x) = \phi_g(y) \to gxg^{-1} = gyg^{-1} \to g^{-1}(gxg^{-1})g = g^{-1}(gyg^{-1})g$

Therefore $x = y$, i.e. ϕ_g is injective.

Then NTS ϕ_g is surjective:

$\forall x \in G, \exists g^{-1}xg \in G, \phi_g(g^{-1}xg) = g(g^{-1}xg)g^{-1} = g.$

Therefore ϕ_g is surjective.

Since ϕ_g is defined from an action, it is already a homomorphism, and therefore ϕ_g is an isomorphism.

Now since ϕ_g is an isomorphism, $\exists \phi_g^{-1}, \forall x \in G, \phi_g^{-1}(\phi_g(x)) = 1.$

Given $a, b \in G, \phi_g(a) = b$, and assume $|a| = m, |b| = n.$

This means $\phi_g(a)^m = \phi_g(a^m) = 1 = b^m$

Therefore $|b| \leq |a|$.

Similarly $\phi_g^{-1}(b)^n = \phi_g^{-1}(b^n) = 1 = a^n.$

Therefore $|a| \leq |b|$.

This shows that $\forall a, b \in G, \phi_g(a) = b$,we have $|a| = |b|$.

Therefore we have $\forall x \in G, |x| = |gxg^{-1}|$.

We can similarly define a map $\psi_g : A \mapsto gAg^{-1}$ by

$$\forall x \in A, \psi_g(x) = gxg^{-1}$$

First NTS ψ_g is well defined:

$\forall x \in A, \psi_g(x) = gxg^{-1}$ which by definition is in gAg^{-1}. Therefore ψ_g is well-defined.

Then NTS ψ_g is both injective and surjective. Which is similar to what we did for showing ϕ_g is invertible. Therefore $\exists$ a bijection ψ_g between A and gAg^{-1}.

Therefore $|A| = |gAg^{-1}|$

3

(1.7.19)

Let H be a subgroup of the finite group G and let H act on G by left multiplication. Let $x \in G$ and let $\mathcal{O}$ be the orbit of x under the action of H. Prove that the map

$$H \to \mathcal{O} \text{ defined by } h \mapsto hx$$

is a bijection. From this and the preceeding exercise deduce **Lagrange's Theorem**:

If G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$.

This map is by nature surjective.

Only NTS it is injective:

$\forall g, h \in H, gx = hx \to (gx)x^{-1} = (hx)x^{-1} \to g = h$.

Therefore the map is injective and therefore a bijection.

4

(2.2.7)

Let $n \in \mathbb{Z}$ with $n \geq 3$. Prove the following:

(a) $Z(D_{2n}) = 1$ if n is odd

(b) $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$.

Given $s \in D_{2n}$, we have

$$\begin{aligned} \forall sr^i \in D_{2n}, sr^i s(sr^i)^{-1} &= sr^i sr^{-i} s \\ &= sr^{2i} \end{aligned}$$

$sr^{2i} = s \to r^{2i} = 1 \to 2i = n$ or $i = 0$ since n is odd, it can only be that $i = 0$, i.e. $sr^0 = s$.

However $sr^i s^{-1} = r^{-i}$. Therefore $\nexists sr^i \in Z(D_{2n})$

Similarly,

$$\forall r^i \in D_{2n}, r^i sr^{-i} = r^{2i} s$$

$r^{2i} s = s \to r^{2i} = 1$ and we can see that r^{2i} must be 1.

This shows that only 1 is in $Z(D_{2n})$ when n is odd.

Using the same logic from above, we can see that when $n = 2k$, we can let $i = k$ so that $r^i = r^k \in Z(G)$.

Therefore $\{1, r^i\} = Z(G)$ when $n = 2k$.

5

(2.2.10)

Let H be a subgroup of G and any nonempty subset A of G define $N_H(A)$ to be the set $\{h \in H | hAh^{-1} = A\}$. Show that $N_H(A) = N_G(A) \cap H$ and deduce that $N_H(A)$ is a subgroup of H.

First NTS $N_H(A) \subseteq N_G(A) \cap H$:

$\forall h \in N_H(A)$, since $h \in H \leq G$ and $hAh^{-1} = A \to h \in N_G(A)$.

Therefore $h \in N_G(A) \cap H$, i.e. $N_H(A) \subseteq N_G(A) \cap H$.

Then NTS $N_G(A) \cap H \subseteq N_H(A)$:

$\forall h \in N_G(A) \cap H$, since $h \in H$ and $hAh^{-1} = A$, $h \in N_H(A)$.

Therefore $N_G(A) \cap H \subseteq N_H(A)$.

Therefore $N_G(A) \cap H = N_H(A)$.

Since $H \leq G, N_G(A) \leq G, \to N_H(A) = N_G(A) \cap H \leq G$.

Since $N_H(A) \subseteq H, \to N_H(A) \leq H$.

6

(2.3.17)

Find a presentation for Z_n with one generator.

$Z_n = \{z | z^n = 1\}$

7

(2.3.25)

Let G be a cyclic group of order n and let k be an integer relatively prime to n. Prove that the map $x \mapsto x^k$ is surjective. Use Lagrange's Theorem to prove the same is true for any finite group of order n.

Since k relatively prime to n, this means $gcd(k, n) = 1$.

Therefore $\exists r, s$ such that $rk + sn = 1 \to \forall a \in \mathbb{Z}, ark + asn = a$.

Therefore $x^{ark+asn} = x^a = x^{ark} \cdot 1$, i.e. $(x^{ar})^k = x^a$.

For any finite group of order n:

Given $x \in G$, by Lagrange's Theorem we know $|x||k$ and thus k also relatively prime to $|x|$.

Therefore this is also true for any finite group of order n.

8

(3.1.9)

9

(3.1.32)

10

(3.1.33)